POSITION CLASSIFICATION STANDARD FOR SECURITY ADMINISTRATION SERIES, GS-0080

Table of Contents

SERIES DEFINITION

This series includes positions the primary duties of which 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. Duties involve the management, supervision, or performance of work in: (1) developing, evaluating, maintaining, and/or operating systems, policies, devices, procedures, and methods used for safeguarding information, property, personnel, operations, and materials; and/or (2) developing and implementing policies and procedures for analyzing and evaluating the character, background, and history of employees, candidates for employment, and other persons having or proposed to be granted access to classified or other sensitive information, materials, or work sites.

This standard supersedes the position-classification standard for this series dated June 1962.

EXCLUSIONS

1. Positions which are concerned with using, processing, protecting, or otherwise handling national security information as an incidental function of the principal duties assigned. For example, positions involving the maintenance of files; technical, scientific, or other positions which require working on or with classified information or projects; or other positions the incumbents of which know and apply specific security protective practices only incidentally to the conduct of their main work are classified in the series appropriate for the principal duties.

2. Positions which are principally concerned with directly administering, supervising, or performing (1) work involved in protecting public property, or property in the custody of the Government or (2) law enforcement operations involving the protection of personnel and property, when such duties consist mainly of supervising or performing guard, patrol, or police work, even when such work is primarily concerned with protecting restricted areas, screening access to such areas, and implementing related security controls. Such positions are classified to the Guard Series, GS-0085, or the Police Series, GS-0083, depending on the nature and scope of specific duties and responsibilities.

3. Positions which are primarily concerned with conducting or supervising the conduct of personal background or criminal investigations are classified in the General Investigating Series, GS-1810, or the Criminal Investigating Series, GS-1811.

4. Positions requiring substantive subject-matter knowledge which are concerned with advising security specialists about or personally classifying information or material into appropriate security categories (confidential, secret, etc.) or with declassifying such material are classified in the appropriate subject-matter series.

5. Positions which require either the performance of work requiring a qualified attorney, or clerical work in support of such legal work, are classified in the appropriate series in the Legal and Kindred Group, GS-0900.

6. Positions which have as their primary concern applying the principles and practices of human resources administration, including resolving questions of suitability for positions based on personal qualifications, are classified in appropriate series in the Job Family Position Classification Standard for Administrative Work in the Human Resources Management Group, GS-0200.

7. Positions the primary duties of which require professional or technical knowledge of the electronic or electrical circuitry of security equipment in order to evaluate, install, maintain, or repair such equipment are classified in the appropriate engineering series or an appropriate technical, repair, or equipment analysis series, such as the Engineering Technician Series, GS-0802.

8. Positions involving responsibility for information technology systems and services used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, assurance, or reception of information. Such positions are classified in the Job Family Position Classification Standard for Administrative Work in Information Technology Group, GS-2200.

9. Positions concerned with analysis, evaluation, and production of reports and estimates from raw intelligence information for purposes of informing others about world events and foreign activities, or for counterintelligence analysis, are classified in the Intelligence Series, GS-0132.

10. Full-performance level (nontrainee) positions evaluated below grade GS-9 which require a fundamental understanding of security information, methods, and procedures, but do not require knowledges characteristic of this series. Such positions are most often performing one-grade interval work in support of security specialists and are classified in the Security Clerical and Assistance Series, GS-0086.

OCCUPATIONAL INFORMATION

Security administration in Federal agencies includes a number of functional areas, particularly personnel, physical, information, and industrial security. (Industrial security includes aspects of the other security functions and applies to industrial and academic organizations under contractual agreement to comply with Federal security requirements.) Security administration involves the safeguarding of information, personnel, property, assets, and/or material from theft, loss, misuse, fraud, disclosure, espionage, or sabotage. It also assures that the employment of personnel in sensitive positions or access by employees and others to secured information, assets, and material is clearly consistent with position sensitivity and in the national interest (national defense, national security, or national resource protection). Security specialists

develop, evaluate, and implement security program policy and/or direction. Some prepare classification guidance, and some make original classification, declassification, downgrading, and upgrading decisions. Many security specialists train security and subject-matter personnel in security requirements and procedures.

Security administration is a specialized and integral aspect of agency missions and programs. It is concerned with (1) identifying the need for protection and security, (2) developing and maintaining the physical means which are used for protection and security, (3) developing, implementing, and maintaining procedural and technical methods to enhance physical protection, (4) assessing the reliability, loyalty, suitability, and trustworthiness of those persons who have access to sensitive or classified information, resources, and material which could adversely affect the national security, the public welfare, or the efficiency of the Federal service, and (5) assessing the damage done to national security when information or material has been compromised or sabotaged. Security administration is concerned with safeguarding information and material whether it is in the direct custody of the Federal Government or in the hands of other governments, private businesses (e.g., those having contacts with the Government), educational institutions, or other persons or organizations.

Information and material, particularly that affecting the national security or the public welfare, may be in any of a wide variety of forms. It may exist in documentary or electronic form, or as materials, hardware, equipment, electronic, magnetic, telemetry, special nuclear materials (weapons, fuels, etc.), money, office equipment, medical supplies, narcotics, industrial or other processes, or even as ideas or concepts in the minds of individuals. The multiplicity of forms of classified or sensitive information and materials helps to emphasize the fact that security administration, as covered by this series, is part of a total protective program required in most Government agencies, installations and industrial facilities. Security programs vary widely in scope, complexity, and purpose. They may, for example, serve primarily to provide protection from loss, unauthorized disclosure, espionage, terrorism, sabotage, natural disaster, or compromise of information or material which is considered vital to national defense and security, as well as to the privacy of individuals and entities. In addition, the protection program may include protection of the agency, its staff, and its premises from intrusion, trespass, acts of violence, theft, or fire.

Security specialists interpret or develop general policy direction for application on an organization-wide basis and conduct oversight reviews on the effectiveness of programs and practices within lower echelon and supported organizations. At operating component, regional, or installation levels, specialists further interpret and define policy guidelines, develop and implement specific guidelines to meet localized requirements, and monitor program effectiveness in Federal, government contractor, and private sector facilities. Security specialists commonly participate in program and project planning efforts to evaluate the need for security requirements and recommend equipment, methods, procedures, and systems. In this role, specialists will sometimes maintain rather substantial budgets for the purchase and installation of security equipment, systems, and services.

Security specialists frequently review intelligence and counterintelligence reports, assess security vulnerabilities, and design security systems based on their analysis of the intent and

operating techniques of hostile intelligence and security services and terrorist organizations. The results of such analyses are used in security program planning, implementation, evaluation, and modification efforts. Some specialists use that information in planning for and participating in programs designed to protect personnel and/or highly sensitive facilities, such as those containing nuclear weapons and other special nuclear materials. Some specialists are trained for and participate in emergency reaction teams, such as those for executive protection or terrorist attack or other kinds of response teams which require training in weapons proficiency and military assault tactics.

Many security specialists perform instructional duties as part of their program responsibilities. Instruction may be provided to other security personnel, subject-matter or contractor employees, or others.

Sometimes the nature and difficulty of the work are affected by the environment in which it is performed. Some security specialists, for example, perform their work in foreign countries where threats of terrorism, the reliability of the local police and military forces, electrical power, water supply, and other factors must be evaluated as a function of developing and implementing security plans. Some specialists work in outdoor environments, sometimes in rough terrain, where the facilities or materials requiring protection are exposed to the elements and/or acts of vandalism, and are so isolated that personal observation and detection is often impossible. Terrain and other geographic factors are often of concern to security specialists in determining appropriate levels for guard forces, the number and placement of detection devices, developing response times for guard and police forces, and similar considerations. The nature of the materials under protection must also be considered in security planning, along with balancing the costs or security systems between the ideal and what can be realistically accomplished.

Some security specialists at the local installation level set up and monitor internal security programs that are administered by subject-matter employees. Such programs include instructions and procedures for controlling and storing documents, office closing procedures, and locking and unlocking procedures for safes, doors, vaults, and desks. Frequently, the performance of such security practices is left in the hands of personnel working in a subject-matter area. The security specialists monitors the operating effectiveness of such programs by administering a system for reporting violations and recommending corrective actions in prescribed security procedures.

Some security specialists are involved in planning for and administering law enforcement and related protective programs (guard services) for Federal agencies and installations. This function is typically part of a physical security program where the protective force is another part of a broader system of security responsibilities. Security specialists plan and advise on staff levels, operational policy and plans, budget and related administrative and doctrinal guidance for protective forces. Direct day-to-day administration and supervision over such work is usually the responsibility of police or guard supervisors.

Nature of Security Work

National security policy is based in legislation and Executive orders. Further policy guidance is developed and issued under the cognizance of the Secretaries of State, Defense, and Energy, the Attorney General, the Director of Central Intelligence, and the National Security Council. Agency security directors and specialists interpret, evaluate, and implement general policy direction and establish an operational framework for security programs. Work assignments of security specialists may be very broad or narrow, covering a single functional area or several, and may concentrate on one or more of the specific subject-matter areas.

Personnel security, to the extent possible, assures the loyalty, reliability, suitability, and trustworthiness of applicants, employees, and others who work with, will work with, or have access to sensitive or classified information and material. *Physical security* is concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. Physical security also provides the criteria for the levels and types of armed security forces required for response and containment. *Information security* is that aspect of security work concerned with identifying materials, processes, and information that require protection and recommending the level of security classification and other protections required. This area also includes the coordination necessary to identify items of information, technology, and materials that are restricted from transfer to foreign nations. *Industrial security* builds on aspects of personnel, physical, and information security for work which takes place in the private sector or in Government-owned/contractor operated facilities. Each of these basic functional areas is further described in the following sections.

Security specialists also perform work in a variety of technical security programs. These include specially tailored security requirements and processes to protect special nuclear materials (research and development laboratories, weapons grade materials, fuels, weapons, reactors, and the related processes for making or using such materials), automatic data processing, agency operations (operations security), electronic emanations, cryptographic materials, and sensitive intelligence information. Participation in these security programs might be part of a broader set of security responsibilities, or might be the only program in which the specialist works. Some of these specific program areas are discussed in the section entitled Specialized Security Assignments.

Personnel Security

This functional area includes those security specialists primarily concerned with formulation and application of security policy, procedures, systems, and programs involving the loyalty and reliability of people. Personnel security specialists determine the suitability and security eligibility of individuals for entry and retention in sensitive and nonsensitive positions. They make security clearance determinations for employees or other persons for access to sensitive information, resources, material, or work sites. The duties include developing and implementing policies and procedures for the personnel security program within the agency or organization,

reviewing requests for security clearances and special accesses, interviewing nominees or applicants, affording rights to due process through hearings when necessary, applying agency or organizational regulations regarding the type of personal security check required (i.e., national agency check, special background investigation, etc.) and requesting an investigation from the appropriate organization.

In carrying out personnel security work, the specialist performs such tasks as evaluating the sensitivity determination for each position, as described by management based on need-to-know principles; determining national security or agency information access requirements; negotiating with organization officials to keep at a minimum the number of positions for which access to national security information is required; developing and implementing procedures and criteria for determining the sensitivity of positions; and determining whether special investigative requirements apply.

Personnel security specialists review, evaluate, and adjudicate reports of investigations, personnel files, and other records to determine whether to grant, deny, revoke, suspend, or restrict security clearances consistent with national security and/or suitability issues. They determine the adequacy and completeness of the investigation and of other means by which data were collected; evaluate the authenticity, veracity, and pertinence of the data to the case at hand; and request additional investigations or develop other information if needed. Security specialists recommend or decide whether security clearances should be granted, suspended, revoked, or denied. Prior to a final adverse employability or security clearance determination, security specialists provide individuals with a comprehensive, written statement of the reasons why employment cannot be offered, security clearances cannot be granted, or adverse action is being taken and consider any response furnished by individuals. In the event eligibility for employment in a sensitive position or a security clearance must be questioned or cannot be granted, security specialists may negotiate with agency, organizations, or industry management on a variety of means for reducing risks of compromise. These may include such factors as the possibility of changes in duties, position location, need to know, need for access to restricted areas, changes in restricted areas, installation of security safeguards, or other approaches to limit access to individuals and, thus, reduce the risk of compromise.

Personnel security specialists provide authoritative information and assistance to organization officials by: advising on personnel security policies and related matters and on the impact of personnel security requirements on organizational missions; formulating and recommending personnel security investigative requirements; advising on procedures for adverse security determinations and employee rights; representing the organization in personnel security matters; developing guidelines, procedures, and other materials for use by operating officials; administering programs for continuous security evaluation of personnel; assisting in arranging and conducting hearings or appeals; and administering security awareness programs. Specialists also advise management on matters about reinvestigation requirements, personnel assurance programs (i.e., ongoing checks on employee reliability), and related matters concerning the maintenance of current clearances and monitoring the reliability of the work force.

Some specialists interview applicants to resolve questions concerning derogatory information developed during the investigation. Personnel security specialists may testify at formal hearings

regarding the clearance processes, criteria, and justification for adverse decisions, or represent their office in inter- or intra-agency meetings concerning personnel security matters.

Some personnel security specialists apply policies and procedures for special access programs and administer military and civilian personnel programs for acceptance, retention, appointment, or elimination from employment or military service. They also advise subject-matter managers concerning policies involving special access security requirements for certain sensitive positions, military specialties, or other assignments.

Physical Security

Work in this security function is concerned primarily 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. Physical security specialists develop security policy and design, develop, evaluate, and sometimes install protection systems and devices to insure that sensitive information, equipment, and other material is not compromised, sabotaged, stolen, misused, or subjected to terrorist, malicious mischief, or other acts of willful interference.

In carrying out these functions, security specialists: review designs; inspect facilities where sensitive material will be located; ascertain the use to be made of material in the organization, who is to use it, and how it should be protected; evaluate the effectiveness of existing security practices; recommend the type of control requirements, procedures, and facilities needed; assure that organization personnel are adhering to established policy and practices; and recommend appropriate action to correct deficiencies. They determine or recommend the number and kind of safes, alarms, locks, fences, and markings needed; lay out restricted or controlled areas; set up personnel circulation, control, and entry systems; and develop procedures for the movement and handling of sensitive material. They also recommend the use and training of protective forces, guard and detection dogs, crime prevention programs, communications command and control centers, and other measures to identify, reduce, eliminate, or neutralize criminal activity. Some security specialists prepare contract specifications, establish performance standards and instructions, and administer contracts awarded for guard services.

Physical security specialists must have knowledge of the state-of-the-art in intrusion detection systems and devices, safes and other storage containers, locks and locking systems, personnel entry control systems, security measures applicable to transporting and shipping requirements, ballistic protection measures, protection levels for special nuclear materials, asset protection, and loss prevention. They must be able to read, understand, and evaluate site/facility engineering drawings for potential security deficiencies and to design and implement installation security systems for new facilities.

Physical security specialists conduct surveys and analyses to identify how critical and vulnerable facilities or sites are and threats against them. They consult with operating personnel and other security specialists to devise protection systems which provide maximum security with the least interference in the organization's mission. This requires, in addition to knowledge of their own

specialized areas, understanding the work and functions of a variety of organizations; the ability to resolve problems or conflicts between physical security requirements and organizational missions; the ability to adjust security systems for multiple and, sometimes, conflicting requirements; the indoctrination and training of organization personnel in the need for observing security requirements; the installation of inventory and control procedures to assure that protected material is accounted for; and ability to review law enforcement and security guard procedures and functions to assure that required personnel are available and material controls are being properly enforced.

Specialists performing physical security work inspect, analyze, and evaluate security systems. They determine, by appropriate tests or otherwise, if the system is providing adequate protection; assess the adequacy of inventory and management control systems; monitor the manner in which sensitive material is handled and used; recommend appropriate corrective action where security requirements are not being observed; and make adjustments in the physical security system as needed.

Some security specialists are involved in integration of security considerations and systems as a function of construction and acquisition planning and execution. This includes protecting against security vulnerabilities that will exist during the development processes as well as those that will require preventive measures on completion of construction or delivery of systems and products.

Information Security

This security function concerns primarily the classification, declassification, and protection of classified national defense and other sensitive information originated or controlled by Federal agencies. It is concerned with identifying information requiring protection and designating the level of protection required. Such information (documents, materials, devices, industrial processes, systems, etc.) is commonly contained within Federal facilities and systems, although it may be located also in industrial facilities, academic institutions, other governmental organizations (including foreign governments), or other locations.

Duties include developing, implementing, and monitoring policies, instructions, procedures, control systems, and methods for such functions and activities as: delegation and exercise of classification and declassification authority; development of classification guides, document marking, safeguarding, and use; personnel access controls; need to know criteria; physical storage and control; security education; and transmitting, transferring, reproducing, downgrading, and destroying information. Specialists also perform oversight reviews to monitor program implementation and practices in those areas by lower echelons and other supported organizations. Performance of this work commonly requires coordination with scientific, technical, and other subject-matter specialists to assess risk of loss, value of loss, and the classification level appropriate to information sensitivity.

Some specialists review plans for proposed or new projects to assure the presence of adequate planning for information security and other controls. This involves determining who should have classification authority and reviewing plans for document and access controls, transmission of sensitive information and materials, and related information controls and safeguards. This process often includes consulting with appropriate officials to determine whether a proposed classification level is too high or too low and whether adjustments are required in control and storage plans. Classification guidance generated for new or ongoing programs is reviewed by specialists to insure that specific and correct guidance is available to users. This work requires knowledge of the subject matter in order to distinguish various levels of classification for existing and proposed new information. During the course of a contract or project, classification control plans are periodically reviewed to determine whether they are current with the information and materials to be protected or need adjustment because of changes in the projects.

Some information security specialists are concerned with developing, implementing, and monitoring procedures for complying with restrictions on transferring technological information to other nations. This includes information contained in reports or other documents which, except for the sensitive information itself, may be released in part to others. It also includes equipment that is integrated into other systems such as military aircraft, computer systems, nuclear technology, weapons systems, and others. The specialist maintains knowledge of such information and systems and changes in their status. They make limited changes in restrictions so information may be released to one country but not to others, and monitors the precautions taken to protect such information from unauthorized transfer.

Some information security specialists are primarily concerned with evaluating foreign government eligibility to receive classified and controlled information. They ensure that decisions to release such information are in the best interests of the United States. They review requests from foreign governments or from other Federal and non-Federal individuals or groups for classified or controlled unclassified information and make determinations about the releasability of the requested information or technology. They also process foreign government and other requests for accreditation to receive or export such information.

Industrial Security

Industrial security work requires many of the knowledges and skills needed to perform personnel, physical, and information security work. Industrial security specialists establish, for each contractor and subcontractor, criteria covering such matters as: foreign ownership or influence; classification and clearance levels required for contract performance; product classification; need for restricted nuclear data; and access to communications security, intelligence or international organization information.

Industrial security specialists conduct surveys of industrial or other private facilities to determine the organization's eligibility to work with and store classified and sensitive information. These surveys involve thorough examination of business documents and personal interviews to: determine the actual ownership or source of control of the organization and organizational

history; identify the organizational structure to include nature of business as well as identity of key officials; assure clearance levels for officials commensurate with information handled; and assess the facilities' physical acceptability for possession of classified and/or sensitive information.

Also included is responsibility for orienting the contractor to the security program and assisting in initiating the measures necessary to bring a facility up to established standards. Industrial security specialists may also negotiate formal security agreements with contractors, process organizational and personnel clearance actions, determine from investigative and other data the kinds of clearance actions to be initiated, and determine if a facility is under foreign ownership, control, or influence.

Industrial security specialists review the nature of classified contracts to identify the level and kind of secure work to be performed in the facility and the kind and extent of security protection required for the programs involved. They work with subject-matter specialists in developing statements of need, descriptions of work, and other considerations relating to the security requirements under a contractual arrangement. They assure that security is considered in the earliest stages of procurement planning and that all requirements are fulfilled. They work with contracting officers to assure that bidders can meet security requirements of the contract. They attend preaward and pricing conferences to assure that security costs are not excessive and assist the contracting office in carrying out security responsibilities.

Industrial security specialists develop security plans involving: access to grounds by employees, vendors, Government personnel, and others; badge and pass systems; clearance records and controls; fences; alarms; intrusion detection and other electronic devices; guard force levels and their duties, responsibilities, and response times; special room construction including vaulting, shielded cable, and wiring requirements; and other means of limiting entry (locks, vaults and safes) or technical penetration (electronic emanations, eavesdropping, or others). The specialist resolves issues with industry officials involving security plans and makes adjustments based on costs, alternative methods available, other security programs in place, and similar considerations.

Industrial security specialists conduct continuing inspections of facilities possessing sensitive information to assure adherence to security requirements. They perform periodic reviews of facilities and their personnel to assess protection against espionage; investigate suspected security violations; and recommend or take appropriate measures to correct security deficiencies, up to and including removal of classified material from the organization's possession or stopping work operations when a significant breach of security is probable. They plan, organize, and conduct training programs to make facility personnel aware of security matters and procedures and to alert them to dangers of espionage and sabotage. Industrial security specialists are responsible also for periodic inspections of private organizations to determine whether the organizations still have need for active facility clearances, and to keep at a minimum the number of authorized personnel clearances by restricting as much as possible the need-to-know.

Industrial security specialists may represent a number of Government agencies in the facilities to which they are assigned. As a consequence, the specialists must be aware of the variety of contracts in the facilities, agency officials responsible for the several programs, and any special

program requirements affecting security matters. They consider the variables introduced by such conditions and present plans for compliance to the contractor.

Specialized Security Assignments

Some security specialists perform security work that is directed toward protecting highly defined information, materials, equipment, or processes by applying specifically tailored security criteria. They use knowledges, skills, and abilities derived from the four basic functional areas of security in combination with supplemental training and experience needed for specialized program requirements. These include protection programs for nuclear materials, data processing facilities, communications centers, cryptographic materials, intelligence operations and information, military operations, and others where the loss of the information or materials could pose a direct threat to national security or to public health and safety.

Each situation requires careful analysis of intelligence and related information to assess vulnerabilities and to design, implement, and evaluate security plans. Such work typically involves comprehensive evaluations of the need for various levels of information, physical, and personnel security. If performed in a private- or Government-owned/contractor operated facility, it also involves the application of industrial security concepts, methods, and techniques. Typically, such programs involve additional restrictions beyond those found in some other security programs, including more refined need-to-know and security clearance criteria, highly specific minimums for physical and electronic barriers, and special control processes for information and documents.

Depending on the assignment, specialized security work may be full time or a part of broader security responsibilities. Nonetheless, the work typically requires knowledge of both basic security concepts, methods, practices, and procedures *and* those that apply specifically to the information, program, facility, or material involved.

Operations security (found primarily in the Department of Defense) is designed to deny information to hostile military and intelligence services about planned, ongoing, and completed military operations. Casual conversation, deviation from routine practices, changes in priorities, intensification of troop movement or logistic support, and the nature of activities, configuration, or location of material can cause speculation by the media, the general public, and hostile intelligence services. When analyzed, these seemingly innocent kinds of activities may point toward and tend to compromise classified information, projects, or programs. Security specialists engaged in operations security conduct comprehensive surveys and analyses of operational functions to determine what needs to be protected, identify and assess the degrees of vulnerability, and select or design appropriate countermeasures that will provide the necessary level of protection against compromise or technology transfer. Specialists use technical knowledge of organizational and management functions in combination with knowledge of the work in the primary security specializations to assess and improve security systems and controls and correct vulnerabilities not covered by traditional security programs. Protection measures must be defined in relation to the degree of risk which can be tolerated and the balance between operational efficiency and cost effectiveness.

Nuclear security involves accounting for and protection of nuclear information, processes, reactors, weapons, fuels, and other nuclear materials. The nature of the information and materials involved, potential losses to national security, and the threat to public health and safety require specific, stringent security programs to prevent their misplacement, loss, theft, misuse, sabotage, or destruction. Specialists in nuclear security apply the concepts, methods, and systems of the basic security functions in designing, implementing, evaluating, and modifying nuclear security programs. This work is performed on Federal property, in contractor facilities, Government-owned/contractor operated facilities, laboratories, academic institutions, or other locations.

Sensitive Compartmented Information (SCI) security involves specialized security programs for intelligence related information and systems under the cognizance of the Director of Central Intelligence. The work can be one element of a broad security program or, because of the size of facility and/or volume of materials involved, may be a full-time assignment. Security specialists may be designated as special security officers by appropriate authority.

Automation (ADP) security is intended to prevent the penetration of computer systems for espionage, sabotage, or fraudulent purposes. Penetration of unprotected systems is possible in a variety of forms including direct access, electronic or other forms of eavesdropping, interpreting electro-mechanical emanations, electronic intercept, telemetry interpretation, and other techniques designed to gain unauthorized access to ADP information, equipment, or processes. Security specialists recognize such potential and, in coordination with technical specialists, define vulnerabilities and oversee the installation of physical and technical security barriers to prevent others from improperly obtaining such information.

Computer programming, encryption, and shielding often require the expertise of specialists in data processing or communications to install software and technical protective systems. Normally, the possession and application of such technical knowledge would constitute the paramount qualification for such positions and cause them to be classified to the appropriate subject-matter series (e.g., Computer Science, GS-1550, or Engineering Technician, GS-0802). In some instances, employees with such technical qualifications may work on broader aspects of security administration and it may be appropriate to classify their positions to the Security Administration Series. The primary purpose of the positions, the paramount qualifications required, and the career path involved are the major considerations in making the proper series determination.

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.

AUTHORIZED TITLES

Personnel Security Specialist, *Physical Security Specialist*, or *Information Security Specialist* is the prescribed title for positions primarily concerned with performing personnel security, physical security, or information security work as described above. Such work may be performed in Government, contractor, or other facilities.

Industrial Security Specialist is the prescribed title for positions performing industrial security work as described above. Industrial Security Specialists are typically concerned with two or more functional security areas (personnel, physical, information) defined in the preceding paragraph. Positions primarily concerned with performing work in one of the functional security areas should be titled in accordance with the preceding paragraph.

Security Specialist is the prescribed title for positions primarily concerned with performing security administration work which does not fall into one of the above specializations. This would include positions performing work in two or more functional security areas other than in industrial security.

In addition, agencies may supplement these prescribed titles by adding parenthetical titles where necessary to identify further the duties and responsibilities involved, where such duties and responsibilities reflect specific knowledges and skills required to perform the work. Possible parenthetical titles include (Operations), (Nuclear), or (ADP).

Positions which meet the criteria of the General Schedule Supervisory Guide for titling as supervisors should have *Supervisory* prefixed to the basic title.

Security Officer is the authorized title for positions responsible for the development, installation, and management of a security program for a governmental organization, organizational segment, installation, or other unit, subject at the local level only to administrative supervision and control. (Policy and technical guidance may be received from a higher organizational entity.) There can be only one Security Officer for an organizational unit.

GRADING POSITIONS

Nonsupervisory security administration work should be evaluated on a factor-by-factor basis, using the factor level descriptions provided in this standard. Only the designated point values may be used. For more complete instructions on evaluating positions, see the Introduction to the Position Classification Standards.

Positions which meet the criteria of the General Schedule Supervisory Guide for evaluation as supervisors should be evaluated by the criteria in that guide.

Grade levels of Security Officer positions can be established using the criteria in this standard, the General Schedule Supervisory Guide, or through cross-series comparison to standards for other series which cover program management functions.

GRADE CONVERSION TABLE

Total points on all evaluation factors are converted to General Schedule grade as follows:

GS Grade	Point Range
5	855-1100
6	1105-1350
7	1355-1600
8	1605-1850
9	1855-2100
10	2105-2350
11	2355-2750
12	2755-3150
13	3155-3600
14	3605-4050
15	4055-up

FACTOR LEVEL DESCRIPTIONS

FACTOR 1, KNOWLEDGE REQUIRED BY THE POSITION

Factor 1 measures the nature and extent of information or facts which the workers 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. To be used as a basis for selecting a level under this factor, a knowledge must be required and applied.

Level 1-5 -- 750 Points

In this level, employees, typically in training or early developmental stages in security work, acquire and use knowledge of the basic principles, concepts, policies, practices, and methods of security administration in one or more of the security functional specialties. They perform elementary developmental and procedural functional specialties. They perform elementary developmental and procedural assignments or operations. Employees at this level commonly assist other security specialists and/or perform highly structured, independent assignments such as:

- Reviewing requests for personnel or facility security clearances to assure that all required information is provided, requesting missing information from the originators, and granting clearances when derogatory information is absent.

- Reviewing reports of personnel investigations to identify the presence or absence of derogatory information and, with more experienced specialists, reviewing the impact of various kinds of derogatory information on the granting, denying, or revoking of security clearances.

- Assisting experienced specialists in conducting onsite physical or industrial security inspections or assistance visits and assisting in the evaluation of findings and development of recommendations for changes.

- Reviewing requests for information security guidance or assistance, identifying the nature of issues involved, and researching guidelines to identify the general policies and procedures that apply to their solutions.

Level 1-6 -- 950 Points

Employees at this level, in addition to the kinds of knowledge required at level 1-5, apply practical knowledge of commonly applied security principles, concepts, and methodologies in carrying out assignments and developing skills by performing limited independent work. The nature of the assignments require some application of judgment in the use of security knowledges and the employee must develop skill 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.

Employees use knowledge of criteria, equipment, or techniques for at least one area of security specialization (personnel, physical, etc.) to resolve well-defined questions or conditions. At this level, the employee uses knowledge of standardized applications or established variations in security criteria involving considerations such as clearance level required, adjudication of security clearances when clear-cut derogatory information is present in the investigative information, nature of materials or information to the protected, cost-benefit relationships for security devices or equipment systems, and similar considerations.

Some employees at this level use knowledge of security programs, methods, and techniques to serve as participants in meetings and ad hoc committees developing local implementing plans and instructions based on well-defined objectives and using fully established methods and procedures.

Some employees use knowledge at this level to serve as team members performing security surveys, and/or in planning and implementing specific assignments that comprise part of an overall security plan and the installation of security systems. Such assignments typically involve coordinating with other members of the team and, perhaps, security and subject-matter specialists concerned with other, related security systems which may impact on the plans and recommendations of the team. The work at this level includes such duties as:

- 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.

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

- Collecting information, interviewing workers, observing physical conditions and related activities concerned with violations and compromises.

- Determining eligibility for access to classified or sensitive information and granting personnel security clearances/accesses in the presence of minor derogatory information (e.g., traffic violations, misdemeanors at least 5 years in the past, and similar situations).

Level 1-7 -- 1250 Points

Employees use knowledge, in addition to that at the lower levels, of a wide range of security concepts, principles, and practices to review independently, analyze, and resolve difficult and complex security problems. Such work situations may involve, for example: conflicting testimony or sources and degrees of significant information in clearance adjudication cases; 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; adjudicating complex personnel security clearances and/or developing guidelines for applying general criteria covering derogatory information that requires extensive experience and personal judgment to resolve; or planning and recommending the installation of multilayered security systems which may involve personnel access controls, physical protection devices, monitoring equipment, security forces, remote alarm equipment, and other measures.

At this level, employees often use knowledge of security program interrelationships to coordinate the objectives and plans of two or more specialized programs; make accommodations in study or survey recommendations to allow for differing program requirements; develop and/or implement procedures and practices to cover multiple security objectives; serve on inter-agency or inter-organization committees and groups to identify and resolve, or to assign responsibilities for resolving, security issues; or to perform similar work. 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.

Many employees use knowledge of a great variety of state-of-the-art security equipment and devices in planning and implementing protective methods and security procedures. These include: fencing variations; a variety of alarm and detection devices; closed circuit television systems; locking devices for doors, windows, vaults, and gates; shielding for cables carrying ADP, communications, and other electronic impulses that might be translatable or make a facility vulnerable to penetration; computer security software; personnel control systems such as various visual and electronic badging systems; and other approaches that are designed for or applied to protecting personnel, equipment, facilities, information, processes, or signals.

This level of knowledge is used also in security program planning at a major organizational level when such work involves applying policy direction to specific operating requirements and developing guidance for applying security policy, procedures, techniques, equipment, and methods to a variety of work situations and various degrees or levels of security controls. This knowledge is used further in responding to problems or questions involving implementation of security guidelines at lower levels and in inspecting operating security programs for adequacy, efficiency, and need for improvement. The employee at this level is commonly considered the major authoritative source of security program knowledge for organizations supported by the local security office and for interpreting policy originating from higher organizational levels (or national policy), developing local policy and implementing instructions, providing authoritative interpretations and guidance to management officials and other security specialists at the same and lower levels, and for resolving issues involving conflicting security requirements.

Employees using this level of knowledge commonly consider and apply several alternatives according to the security requirements for highly specific situations, availability of materials, relationships with other protective programs, and cost/benefit considerations. They also consider administrative processes such as the status of funds for a security project; the schedule and rate of progress in construction projects; overlapping requirements to protect the security of the organization as well as the privacy and reputation of individuals in sensitive, delicate, or controversial situations. Such broad range projects often involve specialists in other security

related activities, such as those concerned with detecting and protecting against electronic emanation vulnerabilities, audio countermeasures, computer penetration, and other applying highly technical methods to detection and prevention efforts. Security specialists use knowledge of technical security programs to identify vulnerabilities, and to arrange for appropriate specialists to perform the technical aspects of the work in conjunction with the personnel, physical, and other elements of new or established security programs.

Level 1-8 -- 1550 Points

Employees at this level, having mastered a major area of security specialization or demonstrated mastery of general security administration programs, use comprehensive knowledge of security policy requirements to function as technical authorities in assignments requiring the application of new theories and developments to security problems not susceptible to treatment by accepted security methods, technology, or procedures. In addition to mastery of the specialty area, employees at this level use knowledge of other security specialties in resolving major conflicts in policy and program objectives.

Some employees use the knowledge at this level to perform key decision-making and policy-developing responsibilities in very difficult assignments such as planning for significantly new or far-reaching security program requirements, or leading or participating as a technical expert in interagency study groups for resolving problems in existing security systems and programs requiring innovative solutions. Also characteristic of positions at this level are duties such as advising top level agency security and subject-matter managers on new developments and advances in security techniques in the specialty area; planning, organizing, and directing studies to develop long range (e.g., 5-10 years) studies and forecasts; recommending methods for enhancing efficiency of security systems through modifications and applications of evolving technology; evaluating and making recommendations concerning overall plans and proposals for major agency and interagency security projects; and implementing national level guidance in agency standards, guidelines, or policies for major security programs.

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. 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).

Level 2-1 -- 25 Points

A higher graded employee or the supervisor provides clear, detailed, and specific instructions for the assignments. The employee at this level is typically inexperienced and brings to the attention of others any problems not specifically covered by the instructions. Completed work is closely reviewed for adherence to prescribed procedures and work involving a great amount of detail is often reviewed in progress.

Level 2-2 -- 125 Points

The supervisor provides specific instructions as to approach, methods, and sources of information on new or unusual assignments. Standard operating procedures and applicable precedents largely govern recurring work in the assigned security specialty area. An example would be an assignment to inspect established physical security systems periodically to assure that equipment is operated and maintained according to prescribed schedules and that compliance with entry controls and security force response times are enforced. The supervisor guides the employee in reviewing work to be done and preparing recommendations made by the employee for actions, changes, or additions to existing systems to resolve the security problems or situations, or to enhance systems for new, higher level protective requirements.

The employee uses initiative in independently carrying out assignments which are covered by established procedures. The employee is expected to seek assistance on deviations, problems, and unfamiliar situations that arise.

Finished work is reviewed for technical adequacy, adherence to standard procedures, and compliance with any special instructions.

Level 2-3 -- 275 Points

The supervisor defines the employee's scope of responsibilities and the objectives, priorities, and deadlines. The employee is provided with more detailed assistance in unusual situations which do not have clear precedents.

The employee, having developed competence in the assignment, plans and carries out the steps involved, handles deviations from established procedures, and resolves problems that arise in accordance with agency or local standards, previous training and experience, established practices, or other security controls appropriate to each assignment. Projects typically involve conflicting interrelationships between security and subject-matter requirements requiring investigation and solution by the employee to determine the methods and procedures to use in the 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, information, or facility involved. Techniques used by the employee during the course of the assignment are not usually reviewed in detail.

Level 2-4 -- 450 Points

The supervisor sets the overall objectives and decides on the resources available. The employee consults with the supervisor in determining which projects to initiate, develops deadlines, and identifies staff and other resources required to carry out an assignment.

The employee, having developed expertise in the particular security specialty area, is responsible for planning and carrying out the work, resolving most of the conflicts that arise, integrating and coordinating the work of others as necessary, and interpreting policy in terms of established objectives. The employee keeps the supervisor informed about progress, potentially controversial matters, or developing security conditions or requirements with far-reaching implications.

Finished work is reviewed from an overall standpoint in terms of feasibility, compatibility with other security program requirements, or effectiveness in meeting objectives and achieving expected results.

Level 2-5 -- 650 Points

The supervisor provides broad administrative and policy direction through discussion of financial and program goals and national, agency, and local security policies affecting the direction of the security program.

The employee at this level works under broad delegated authority for independently planning, scheduling, coordinating, carrying out, and monitoring the effectiveness of the operation of the security program(s).

In performing the work, the employee makes extensive unreviewed technical judgments concerning the interpretation and implementation of existing security policy for the assigned specialty area(s) and in deciding which analytical and technical decisions lead to, or form the basis for, major security program policy and operational decisions by top management. The employee is regarded as the leading technical authority for the employing organization in a security specialization or over a wide range of interrelated security programs. The supervisor usually accepts the employee's recommendations without change.

The employee's actions, decisions, and recommendations are reviewed primarily for results obtained in achieving security goals and objectives, and in providing support for the attainment of the organization's mission responsibilities. The supervisor evaluates the employee's recommendations for new or revised security policies, procedures, and controls in terms of impact on subject-matter program goals and objectives, and national security priorities.

FACTOR 3, GUIDELINES

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

Individual jobs in different echelons in an organization, in different work environments, or in different specializations within the occupation use guidelines that vary in specificity, applicability, and availability for performance of assignments. Consequently, the constraints and judgmental demands placed upon employees also vary. For example, the existence of specific instructions, procedures, and policies may limit the opportunity of the employee to make or recommend decisions or actions. However, in the absence of procedures or under broadly stated objectives, employees may use considerable judgment in researching literature and general policy statements, and developing new methods for doing the work which become guidelines for others.

Guidelines should not be confused with the knowledges described under Factor 1, Knowledge Required by the Position. Guidelines either provide reference data or impose certain constraints on the use of knowledges. For example, for a given kind of security requirement, there may be three or four standardized methods for providing the level of security required. A security specialist is expected to know those methods. In a specific installation, however, the policy may be to use only one of the methods, or the policy may state specifically under what conditions one or the other of them may be used.

Level 3-1 -- 25 Points

Specific, detailed guidelines are provided to the employee, as in the case of trainees following detailed procedures, manuals, or checklists in accomplishing routine supportive tasks to develop skills for higher level work and learn about the missions of the security organization.

The employee works in strict adherence to the guidelines. Any deviation from the guidelines and procedures must be authorized in advance by the supervisor or a higher graded co-worker.

Level 3-2 -- 125 Points

Procedural instructions for doing the work have been established by the employing organization or agency and are readily available to the employee. Guidelines cover a wide variety of procedural and administrative conditions, such as: documentation requirements for new or proposed security systems; personal information needed for background investigations and security clearance processes; clearly acceptable information for granting clearances; or marking and storage instructions for classified or sensitive documents, processes, and equipment.

The number and similarity of guidelines requires the employee to use judgment in locating and selecting the proper procedural and technical instructions for application to specific security assignments.

Adaptation of, or deviations from, guidelines are limited to matters of style and format for describing physical and other conditions that affect implementation of security protection systems or costs involved in achieving a required level of security protection. The employee determines which of several established alternative procedures to use in estimating costs for installing security equipment and develops recommendations about which procedures can best satisfy the security objectives in each specific assignment.

Situations not covered by existing guidelines, or for which guidelines are conflicting, ambiguous, or not available to the employee, or which would require significant deviations from existing guidelines, are referred to the supervisor or to a higher graded employee skilled in the work.

Level 3-3 -- 275 Points

Guidelines available and regularly used in the work are in the form of agency policies and implementing directives, manuals, handbooks, and locally developed supplements to such guides, such as building plans, survey schedules, detailed work procedures, and directives that supplement agency directions. The guidelines are not always applicable to specific conditions or there are gaps in specificity in application to specific security system requirements. This level also includes work situations in which the employee must interpret and apply a number of subject-matter policies and regulations such as those that apply to access to and protection of classified information.

The employee uses judgment in interpreting, adapting, and applying guidelines, such as instructions for the application of security alarm and detection equipment; access barriers (badge and pass system, fences, guard posts, etc.); variations in security clearance levels required for portions of projects or facilities; document control systems and storage facilities where there is some overlap or conflict in the levels of security required and the number and clearance levels of persons with access to a facility; and other conditions requiring the employee to analyze and develop security plans within the intent of available guidelines. The employee independently resolves gaps in specificity or conflicts in guidelines, consistent with stated security program objectives.

The employee analyzes the applicability of guidelines to specific circumstances and proposes regulatory or procedural changes designed to improve the effectiveness or efficiency of security controls within the intent of directions concerning the level of security required.

Level 3-4 -- 450 Points

Guidelines provide a general outline of the concepts, methods, and goals of security programs. The guidelines regularly applied at this level consist of broad security guidance, such as directives issued by national security agencies; general agency policy statements and objectives;

interagency security program policy proposals requiring refinement and coordination; or others that are not specific in how they are to be defined, implemented, and monitored.

Where guidelines for performing the work are scarce or of limited use, 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 geographical regions. Typically, departmental guidelines available to the employee at this level are purposely left open to some local interpretation in order to allow accommodation to variations in local and remote environmental conditions that affect the nature of security systems designed to satisfy overall policy direction. Due to the lack of specificity, the guidelines are often insufficient to accomplish specific objectives. 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, statements of policy, and programs needs; or working with program officials to anticipate security requirements and prepare general operating instructions. The work at this level may also include interpretation and preparation of implementing procedures and instructions at field levels based on general agency policy statements. The specialist establishes and monitors 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.). Such work typically involves security requirements that require tailoring of programs to meet special circumstances.

The employee uses initiative and resourcefulness in researching and implementing new and improved security methods and procedures within the employing organization. The employee establishes criteria for identifying and analyzing trends in security violations and other lapses in security, and in measuring organizational effectiveness in achieving security objectives and goals.

At this level, the employee exercises a great deal of personal judgment and discretion with broad latitude for interpreting and applying guidelines across the organization. Also included at this level is the interpretation and application of guidelines of more than one Federal agency or department which apply to security programs and organizations involved in joint responsibility control, and operations, or discrete projects at a single facility.

Level 3-5 -- 650 Points

At this level, the employee is a recognized technical authority on the development and interpretation of security guidelines, policies, legislation, and regulations covering the security operations of one or more substantive national security programs (physical, industrial, personnel, information, etc.) and the organizations which administer them. Guidelines are nonspecific and stated in terms of broad national or departmental policies and goals, often in obscure legal and technical terminology which necessitates extensive interpretation to define the extent and intent of coverage. Some employees interpret national policies, goals, and legislation in developing security guidance and regulations which apply to the conduct of diverse security and subject-matter program operations, Government wide. Some employees develop guidance in the

form of security circulars, directives, or instructions of the implementation of new and revised methods which organizations are required to use in formulating their security programs. Some employees at this level represent their organizations as technical experts on interagency committees and task forces formulating general program guidance for implementation in a variety of different operating environments where variations in methods and techniques may be needed in order to meet particular security program objectives.

At this level, employees must use initiative, judgment, and originality in researching and interpreting existing national policies and legislation, in determining when new or revised legislation is needed, and in researching and preparing recommendations for the content of such legislation. Employees, as recognized technical authorities in one or more security specializations, develop regulations and security policies. They take into account the effects of conflicting laws, policies, and regulations, and they participate in promulgating security policies and regulations which are flexible enough despite changes in security technology to remain current in meeting program objectives.

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.

Level 4-2 -- 75 Points

Assignments consist of duties and responsibilities involving the performance of related steps, methods, tasks, and procedures in one or more of the security specializations. The employee typically works as a trainee or as an assistant to an experienced worker. Assignments usually involve various sequential steps such as gathering information about room and building configurations, reviewing the adequacy of personnel investigation reports, preparing straight-forward information about document inventory and marking procedures, or other tasks which have been screened to eliminate those aspects of the work that are difficult to identify. Typically, there is some choice involved, such as the form in which information is organized or presented, or the selection of a guide appropriate to the assignment.

Actions to be taken are based on clearly applicable documentation requirements and well-established procedures.

Level 4-3 -- 150 Points

Employees perform various duties requiring the application of different and unrelated methods, practices, techniques, or criteria. Assignments characteristic of this level include: developing alternate security plans for a facility describing options in levels of protection and the costs involved for a Federal or private sector facility where the minimum protection requirement is well defined and accepted techniques are appropriate; adjudicating security clearance requests

involving mixtures of such things as derogatory information, applicants or employees with hard to get skills, and management willingness to accept a nominal security risk; defining information storage requirements involving mixes of classified information requiring separate controls for access; or developing security plans involving separate, although similar, protective systems for communications and ADP facilities requiring separate security considerations within an established physical and information security protection system.

Employees compile, analyze, and summarize information relating to the designated security requirements; develop plans for approaches that may be taken; define the level of risk involved for each plan; develop the costs for implementing each of several options; and recommend a course of action to meet assignment objectives.

The work requires consideration of program plans, applicable policies, regulations and procedures, and alternative methods of implementing and monitoring security requirements. Employees identify and analyze relationships among organizational needs and objectives, costs, requirements of security guides, and related information in reports such as mission statements, levels of guard or police protection available, personnel skill requirements, and facility plans.

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 related to the assignment.

Level 4-4 -- 225 Points

Employees perform assignments consisting of a variety of security duties involving many different and unrelated processes and methods relating to well-established areas of security planning and administration. Typically, such assignments concern several broad security program areas or, in a specialty area, require analysis and testing of a variety of established techniques and methods to evaluate alternatives and arrive at decisions, conclusions, or recommendations. Programs and projects may be funded by, or under the cognizance of, different organizations with differing security requirements or variations in ability to fund system implementation. The implementation of established security policies, practices, procedures, and techniques may have to be varied for a number of locations or situations which differ in kind and level of security, complexity, and local conditions or circumstances requiring adjustment or modification in established approaches. Implementation of the results of analysis may have to be coordinated with other organizations and security systems to assure compatibility with existing systems and demands on available resources.

In deciding what is to be done, the employee typically assesses situations complicated by conflicting or insufficient data, evidence, or testimony 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 and investigative standards, or whether specific kinds of waivers can be justified.

Employees make many decisions involving the interpretation of considerable data; application of established security methods, equipment, techniques, and objectives to a variety of situations with variations in the level of security required; and ability to meet or exceed minimal acceptable levels. The employee plans the work, develops recommendations, and refines the methods and techniques to be used.

Level 4-5 -- 325 Points

Employees perform assignments involving various projects, studies, or evaluations requiring the application of many different and unrelated processes, differing regulatory criteria and procedures, and significant departures from established practices, to reach decisions, or to develop and implement new methods and techniques that satisfy policy and operational requirements. At this level, the employee makes recommendations for changes in basic policy issuances and for implementing instructions covering established security techniques, practices, and methods based on personal analysis of very general policy directives and objectives. An example of work at this level would be interpretation and implementation of new directions for subordinate organizations and field units, when such directions stem from additions to, or changes in, national or agency policies and programs, or identification of deficiencies in established programs.

Decisions regarding what needs to be done are complicated by the number and nature of existing security programs or other regulatory guidance or circumstances, overlapping requirements, distinct local, environmental, or other considerations that have an impact on the ability to apply established methods. Many other factors may require extensive analysis and coordination to implement security plans and programs, such as conflicting requirements or objectives that may be imposed by other agencies. The employee must consider probable areas of future change in system designs, equipment developments, or comparable aspects of projects in order to prepare for later changes.

Usually, there are conflicting requirements, the problems are poorly defined or require projections based on variable information or technological development, or some degree of change must be anticipated in mission requirements, related security systems, or funding requirements.

The work involves originating new security techniques, establishing criteria, or developing new information and approaches to problem solutions. Employees who develop and interpret broad security policies and regulations must consider the total range of existing policies, procedures, laws, and regulations and the program goals and objectives which are to be fulfilled.

Level 4-6 -- 450 Points

Employees at this level perform work which involves analyzing, planning, scheduling, and coordinating the development of legislation and security policy issuances that direct the course of security programs across organizational lines in Federal agencies, industrial organizations, academic institutions, or others involved in sensitive and secure work performed in or for the Federal Government. Typically, assignments having such characteristics involve participation,

as an expert authority, resolving problems or issues concerning several phases of security policy development and implementation for a variety of programs in one or more fields of security. Such work often involves overlapping, conflicting, or difficult to resolve security objectives and requirements. Work at this level may also include problem-solving efforts as a member on interagency committees or in national security organizations involved in reviewing, analyzing, developing, and issuing national policy directives and drafting legislation affecting security policies and programs throughout the Government and private sectors.

Decisions and recommendations made by the employee require extensive consideration and analysis of very broadly defined, or undefined, issues and problems, often exploratory in nature, in areas where useful precedents do not exist and establishment of new concepts and approaches is required. Difficulty is also encountered in identifying and recommending alternate ways to resolve conflicting objectives which result from important national programs (e.g., Freedom of Information Act) that may overlap or conflict with equally important national security priorities.

The employee's actions require continuing efforts to establish concepts, theories, or programs, or to resolve previously unyielding problems in establishing and administering security programs. The work requires extensive coordination and support of other experts both within and outside the organization.

FACTOR 5, SCOPE AND EFFECT

This factor covers the relationship between the nature of the work (i.e., the purpose, breadth, and depth of the assignment) and the effect of work products or services both within and outside the organization.

Effect measures such things as whether the work output facilitates the work of others, provides timely services of a personal nature, or has an impact on the adequacy of research conclusions. The concept of effect alone does not provide sufficient information to understand and evaluate properly the impact of the position. The scope of the work completes the picture, allowing consistent evaluation. Only the effect of properly performed work is to be considered.

Level 5-1 -- 25 Points

The employee performs work consisting of specific operations that include a few separate tasks or procedures intended primarily to develop skills to assume more responsible duties. Work performed by the employee facilitates the work of higher graded co-workers within the immediate organization by relieving them of routine procedural tasks in closely directed phases of security work.

Level 5-2 -- 75 Points

The primary purpose of the work is to assist higher grade employees in the performance of detailed and routine work, in order to develop general skills in security administration. The work involves the application of specific, well-established rules, regulations, and procedures in

one of the security specialties or in general security functions, working across the specialized lines of security work.

Work products and services affect the accuracy and timeliness of broader projects or studies being performed by more experienced employees.

Level 5-3 -- 150 Points

The work involves resolving a variety of conventional security problems, questions, or situations, such as those where responsibility has been assigned for monitoring established security systems and programs or performing independent reviews and recommending actions involving well-established criteria, methods, techniques, and procedures.

The employee's work products, advice, and assistance affect the effectiveness and efficiency of established security programs and contribute to the security effectiveness of newly introduced programs and facilities requiring such protective services. The effect of the work is primarily local in nature, although some programs may be part of multi facility or nationwide program operations with interlocking security requirements.

Level 5-4 -- 225 Points

The work involves investigating and analyzing a variety of unusual security problems, questions, or conditions associated with general questions about security or in a specialty area, formulating projects or studies to alter existing security systems substantially, or establishing criteria in an assigned area of specialization (e.g., developing specifications for security programs in a number of data processing centers)

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

Level 5-5 -- 325 Points

Work at this level involves such things as: isolating and defining issues or conditions where a number of project efforts or studies must be coordinated and integrated, resolving critical problems in agency wide systems, or developing new approaches and techniques for use by others. Typically, employees at this level serve as expert consultants in an area of specialization or as project coordinators in carrying out one-of-a-kind projects.

The employee's advice, guidance, or results affect development of major aspects of security program definition and administration throughout the agency. Such work significantly affects the work methods to be applied by other security specialists throughout the agency and often in other agencies.

Level 5-6 -- 450 Points

The work involves planning, developing, and carrying out vital security projects and programs which are central to the mission of the agency and typically of national or international impact. Work on policy matters often involves establishing the agency's position on broad issues or working on national level committees and working groups to develop security programs of importance to national security policy in defense, economic, political, and law enforcement programs. Typical of the work at this level is that of a project leader for a group which includes key representatives from other agencies or departments.

The work is oriented to long-term efforts on new, significantly enhanced, or significantly changed national security programs that will establish precedents in the affected areas and often influence major functions of other agencies and non-Government organizations.

FACTOR 6, PERSONAL CONTACTS

This factor includes face-to-face contacts and telephone and radio dialogue with persons not in the supervisory chain. (NOTE: personal contacts with supervisors are covered under Factor 2, Supervisory Controls). 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 which are essential for successful performance of the work and which have a demonstrable impact on the difficulty and responsibility of the work performed. NOTE: The same personal contacts should be used for both Factor 6 and 7.

Level 6-1 -- 10 Points

Contacts at this level are with co-workers within the employing office and other employees in functionally related support activities. Typically, the employing office is in a security or law enforcement program or other administrative organization in which security work is carried out for a variety of locally serviced activities and components.

Level 6-2 -- 25 Points

Contacts are with persons from outside the immediate employing office or organization, but usually within the same Federal agency or major component thereof. Typical of contacts at this

level are project managers responsible for substantive subject-matter programs or their designated representatives; engineers, chemists, and other technical subject-matter specialists; program analysts; and other security specialists at various levels within the agency, in field or headquarters locations. Roles and relative authorities of participants are explicit, as in the case of a security specialist conferring with the director of a program in order to present optional security plans involving alternative levels of protection, and differing cost factors, or a formal presentation of security recommendations in a meeting with the head of an agency component.

Level 6-3 -- 60 Points

Contacts are with individuals from outside the agency who represent the security program interests of other Federal agencies, contractors, private business and financial interests, State and local governments, foreign governments, public and private institutions (e.g., colleges and universities), or congressional offices. Contacts with applicants and potential contractors to discuss problems concerning the granting of security clearances are also included at this level. Contacts take place in a moderately unstructured setting (e.g., the contacts are not established on a routine basis, the purpose and extent of each contact is different, and the role and authority of each party is identified during the course of the contact).

Also characteristic of this level are contacts with the head of the employing agency, key officials of comparable rank and authority in other agencies, or the staff of national security agencies. Contacts normally take place at formal security briefings, deliberations, conferences, or negotiations which are arranged well in advance. Attendance at interagency committee meetings as a resource person (i.e., to provide technical security information about specific programs) is included at this level.

This level also includes contacts with employees of other Federal organizations engaged in security functions which affect the budget of the employing organization, and contacts with representatives of private firms performing services for the Government which involve security considerations as a function of contract performance.

Level 6-4 -- 110 Points

Contacts at this level 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. This level also includes contacts with presidents of large national or international firms, internationally recognized representatives of the news media, presidents of national unions, State governors, or mayors of large cities.

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.

Level 7-1 -- 20 Points

The purpose of contacts is to obtain or convey information about the security programs of the employing organization. Information exchanged may include such things as the status of funds for a security project; the schedule and rate of implementation of a security system; current security policies and regulations; and/or standardized methods, techniques, and procedures for planning and implementing a security system.

Level 7-2 -- 50 Points

Contacts are made for the purpose of resolving security issues and problems or for carrying out security plans and reviews to achieve mutually agreed upon security and program objectives. Typically, the employee has extensive contacts with program managers and personnel in staff support offices for the purpose of consolidating requests of components or segments of the organization into single or coordinated security plans and similar purposes which involve explaining and coordinating security program efforts. Such contacts may also include those with managers and employees in contractor facilities to plan and coordinate inspections, provide advice, and resolve security issues.

Level 7-3 -- 120 Points

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

Level 7-4 -- 220 Points

The purpose of contacts is to present, justify, and defend, before policy and organizational approving authorities, far-reaching security recommendations and actions such as: proposed legislation; plans to combine, consolidate, or modify major security programs; or the redistribution of security program responsibilities among different departments and agencies. Contacts at this level commonly involve negotiating and resolving controversial security program issues of considerable significance which are not susceptible to resolution at lower

echelons in Government agencies. Some employees act as advocates at the highest level of Government for agency and/or national security programs and policies.

FACTOR 8, PHYSICAL DEMANDS

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

Level 8-1 -- 5 Points

The work is sedentary and is usually accomplished while the employee is comfortably seated at a desk or table. Some walking and standing may occur in the course of a normal workday in connection with travel to and attendance at meetings and conferences away from the work site.

Items carried typically are light objects such as briefcases, notebooks, and data processing reports. Lifting of moderately heavy objects is not normally required. No special physical effort or ability is required to perform the work.

Level 8-2 -- 20 Points

The work requires regular and recurring physical exertion, such as long periods of standing, walking, bending, stooping, reaching, crawling and similar activities. Security specialists engage in such exertions when, for example, they inspect office buildings or industrial facilities, large military complexes or remote sites. Performance of work may take place in attics, crawlspaces, walls, ceilings, and other limited access spaces, in rough terrain or in construction sites when planning and monitoring the installation of security systems as part of original construction. The work may regularly involve lifting and carrying moderately heavy objects of 50 pounds or less when delivering or installing security devices. The work may require some common characteristics and abilities of physical agility and dexterity to work in confined spaces and to move or lift moderately heavy objects.

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. Although the use of safety precautions can practically eliminate a certain danger or discomfort, such situations typically place additional demands upon the employee in carrying out safety regulations and techniques.

Level 9-1 -- 5 Points

The work is primarily performed in an office-like setting involving everyday risks or discomforts which require normal safety precautions typical of such places as offices, meeting and training rooms, libraries, residences, and private or commercial vehicles, using safe work practices with office equipment, avoiding trips or falls, observing fire regulations and traffic signals, etc. The work area is adequately lighted, heated and ventilated.

Level 9-2 -- 20 Points

The work is performed in settings in which there is regular and recurring exposure to moderate discomforts and unpleasantness, such as high levels of noise in contractors' plants, high temperatures in confined spaces, or adverse weather conditions at construction sites. The employee may be required to use protective clothing or gear such as masks, gowns, coats, boots, goggles, gloves, or shields.