DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, DC 20310-1001

REPLY TO
ATTENTION OF

DAMI-CP

17 March 1993

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Clarification of Differences in Work Among CP-19 GS-080, CP-35 GS-080, and GS-132 (in Counterintelligence) Occupations

1. References:

a. Message, HQDA, DAMI-ZD, 161427Z Oct 92, subject: Results of Study to Reclassify and Retitle Security Specialist, GS-080 Positions in Civilian Intelligence Personnel Management System (CIPMS) to GS-132 Intelligence Specialist (Security).

b. Memorandum, HQDA, ODCSPER/ODCSINT, DAMI-CP, 11 Jun 90, subject: Guide to Classifying General Schedule (GS) Positions in the Civilian Intelligence Personnel Management System (CIPMS) and Implementation of CIPMS Primary Grading Standard (PGS) for Supervisory/Managerial Positions.

2. Reference 1a stated the decision made by the Assistant Deputy Chief of Staff for Intelligence to not change the classification of security specialist positions in CIPMS from GS-080 to GS-132.

a. The suggestion for the potential change in series was made at the May 1992 CIPMS Planning Conference. This issue was tasked to the Intelligence Personnel Management Office (IPMO). A steering group of three functional career program managers was formed to consider the benefits, concerns, problems and cautions associated with making the series change. A telephonic survey of CP-35 leaders was included in the study to ensure broad functional insight.

b. Based upon the pros and cons of the concept, the study group recommended against the change. Instead, the group recommended that clarifying guidance be developed to facilitate and standardize judgments when determining the correct series for positions performing the following work: physical security covered by the competitive service in the Physical Security and Law Enforcement Career Program (CP-19); security administration work that is intelligence-related covered by the CIPMS Career Program (CP-35); and counterintelligence work covered by CIPMS CP-35 in the Intelligence Specialist Series, GS-132.

DAMI-CP
SUBJECT: Clarification of Differences in Work Among CP-19 GS-080, CP-35 GS-080, and GS-132 (in CI) Occupations

3. The enclosed document provides guidance designed to elucidate the differences in work described above. The material was developed in partnership with the steering group of functional career managers who conducted the subject study, the Functional Chief Representative for CP-19, and a representation of CP-35 functional leaders. The document includes:

a. A listing of Army publications which relate to work in positions covered by CIPMS CP-35, and nonCIPMS CP-19.

b. Definitions of the Intelligence Career Program (CP-35) and the Physical Security and Law Enforcement Career Program (CP-19).

c. A definition of physical security, extracted from AR 190-13, applicable to CP-19.

d. Regulatory definitions from Army Regulations appropriate to nonCIPMS CP-19 GS-080, CP-35 GS-080 and GS-132 counterintelligence (CI) work covered by CIPMS.

e. Questions and answers designed to resolve definitional problems and clarify differences in work among CP-19 GS-080, CIPMS GS-080, and GS-132 work in counterintelligence.

4. The enclosure should be inserted into reference 1b, the CIPMS Guide for Classifying GS Positions, at Chapter 3, Classification Principles and Practices. A new Table of Contents for reference 1b is not provided. Recommend a pen and ink notation be made on page 1 of the Table of Contents in the Guide as follows: 3-1.c, Definitional Guidance When Choosing the Appropriate Series Among Security and Closely Related Work.

5. Point of contact in DAMI-CP is Mary Tanzer, commercial (703) 285-5202 or DSN 356-5202.

Encl
as

RICHARD H. CHRISTENSEN
Acting Director, Intelligence
Personnel Management Office

DISTRIBUTION:
MACOM/FOA CPDs
MACOM/FOA CPMs
Installation CPOs
Activity CPMs
FCR, CP-19 (Mr. Mota)

UPDATE TO: The Guide to Classifying General Schedule (GS) Positions in the Civilian Intelligence Personnel Management System (CIPMS), June 1990

ADDITION	ISSUE DATE	PAGES
Provides clarifying guidance to facilitate and standardize judgments when determining the correct series for positions performing the following work: ***physical security*** covered by the competitive service in the Physical Security and Law Enforcement Career Program (CP-19); ***security administration*** work that is intelligence-related covered by the CIPMS Career Program (CP-35); and ***counterintelligence*** work covered by CIPMS CP-35 in the Intelligence Specialist Series, GS-132.	17 March 93	File pages 1 through 22 in the CIPMS Guide for Classifying GS Positions, June 1990.

A pen-and-ink change should be made to the Table of Contents in the Guide to record this addition under CHAPTER 3 - CLASSIFICATION PRINCIPLES AND PRACTICES, Pay plan and series determination.

a. This addition should be noted in the Table of Contents and cross-referenced in the Guide as paragraph 3-1.c, Army Regulations (AR), References, and Definitional Guidance To Be Used in Determining the Most Appropriate Series Among Physical Security, Intelligence-Related Security Administration, and Counterintelligence (CI) Work.

b. The transmittal reference is Memorandum, DAMI-CP, 17 March 1993, subject: Clarification of Differences in Work Among CP-19 GS-080, CP-35 GS-080, and GS-132 (in Counterintelligence) Occupations.

c. The update includes the following:

- A listing of Army publications which provide guidance for positions covered by CIPMS CP-35.

- A listing of Army publication which provide guidance for positions covered by Physical Security and Law Enforcement Career Program (CP-19).

- Definition of the Intelligence Career Program (CP-35).

- Definition of the Physical Security and Law Enforcement Career Program (CP-19).

- Definition of Physical Security, extracted from AR 190-13, applicable to CP-19.

- Regulatory definitions appropriate to non-CIPMS CP-19 GS-080, CP-35 GS-080, and GS-132 in counterintelligence (CI) work covered by CIPMS.

- Questions and answers designed to resolve definitional problems and clarify differences in work among CP-19 GS-080, CIPMS GS-080, and GS-132 work in CI.

Enclosure

ARMY REGULATIONS (AR), REFERENCES, AND DEFINITIONAL GUIDANCE TO BE USED IN DETERMINING THE MOST APPROPRIATE SERIES AMONG PHYSICAL SECURITY, INTELLIGENCE-RELATED SECURITY ADMINISTRATION, AND COUNTERINTELLIGENCE (CI) WORK.

The following references and definitions may be used, in addition to guidance in the position classification standards, when determining the most appropriate series among security administration work that is intelligence-related and covered by the CIPMS Intelligence Career Program (CP-35), security work that is related to law enforcement and crime prevention covered by the competitive service Physical Security and Law Enforcement Career Program (CP-19), and counterintelligence work that is covered by CIPMS Intelligence Career Program (CP-35).

REFERENCES:

THE ARMY PUBLICATIONS LISTED BELOW PROVIDE GUIDANCE FOR POSITIONS COVERED BY CIPMS IN CP-35.

AR 380-5
Department of the Army Information Security Program

AR 380-10
Disclosure of Information and Visits and Accreditation of Foreign Nationals

Confidential AR 380-15
Safeguarding Classified NATO Information (U)

AR 380-19
Information Systems Security

Confidential AR 380-28
Department of the Army Special Security System (U)

AR 380-40
Policy for Safeguarding and Controlling COMSEC Information

AR 380-49
Industrial Security

AR 380-53
Communications Security Monitoring

AR 380-67
Personnel Security Program

AR 380-150
Access to and Dissemination of Restricted Data

Confidential AR 380-381
Special Access Programs (SAPs) (U)

AR 381-1
Control and Dissemination of Intelligence Information

AR 381-10
U.S. Army Intelligence Activities

AR 381-12
Subversion and Espionage Directed Against the US Army

Confidential AR 381-14
Technical Surveillance Countermeasures (U)

AR 381-20
U.S. Army Counterintelligence

Secret AR 381-47
U.S. Army Counter-espionage Activities (U)

AR 530-1
Operations Security (OPSEC)
(This regulation may also provide guidance for positions covered by CP-19.)

AR 690-13
Civilian Intelligence Personnel Management System (CIPMS)--Policies and Procedures

AR 195-6
Department of the Army Polygraph Activities
(This regulation may also provide guidance for positions covered by CP-19.)

FM 34-60
Counterintelligence

Secret FM 34-60A
Counterintelligence Operations (U)

THE ARMY PUBLICATIONS LISTED BELOW PROVIDE GUIDANCE FOR POSITIONS COVERED BY PHYSICAL SECURITY AND LAW ENFORCEMENT CAREER PROGRAM (CP-19).

AR 15-15
Department of the Army Physical Security Review Board

Confidential AR 50-5-1
Nuclear Weapon Security (U)

AR 190-11
Physical Security of Arms, Ammunition, and Explosives

AR 190-13
The Army Physical Security Program

AR 190-15
Physical Security of the Alternate Joint Communications Center

AR 190-16
Physical Security (Joint Services Regulation)

AR 190-18
Physical Security of U.S. Army Museums (to be abolished and absorbed by AR 190-11 and AR 190-51)

AR 190-30
Military Police Investigations

AR 190-50
Physical Security for Storage of Controlled Medical Substances and Other Medically Sensitive Items (To be abolished and absorbed in AR 190-51)

AR 190-51
Security of Army Property at Unit and Installation Level

AR 190-54
Security of Nuclear Reactors and Special Nuclear Materials

AR 190-59
Chemical Agent Security Program

AR 195-1
Army Criminal Investigation Program

AR 195-2
Criminal Investigation Activities

AR 195-7
Criminal Investigative Support to the Army and Air Force Exchange Service (Joint Regulation)

AR 525-13
The Army Terrorism Counteraction Program

DA Pam 190-12
Military Working Dog

DA Pam 190-51
Risk Analysis for Army Property

DA Pam 190-52
Personnel Security Precautions Against Acts of Terrorism

DA Pam 190-52-1
Personnel Security Precautions Against Acts of Terrorism Against the Individual

INTELLIGENCE CAREER PROGRAM (CP-35):

CP-35 is defined in AR 690-13, CIPMS--Policies and Procedures, dated 30 September 1990, and in the ACTEDS Intelligence Plan, dated 20 September 1990. Work in this career program encompasses the following groups of Army CIPMS positions:

Intelligence Specialist, GS-132, positions which are involved in counterintelligence investigations, operations, collection, analysis and production functions; also, intelligence and threat support, and intelligence combat developments.

Security Specialist, GS-080 positions which are predominantly (at least 51%) intelligence related. CIPMS intelligence-related work includes the following security functional areas: ***automation, disclosure, industrial, information, operations (OPSEC), personnel, and technical security.*** These functional areas are defined in the CIPMS Army Occupational Guide (AOG) for Security Administration, GS-080, dated June 1991. (Physical security work performed by CIPMS GS-080 security specialists applies to security of classified information or facilities.)

Scientific and technical positions engaged in targeting and/or the engineering, physical, or technical sciences in an intelligence function, assigned to an organizational component performing an intelligence mission. (GS-400/800/1300/1500 occupational groups.)

Intelligence education and training positions which are in intelligence organizations, the duties of which require the incumbent to possess intelligence-related skills, knowledges, and abilities. (GS-1701/1712 occupational series.)

Additional positions in the GS-301 series where the predominant knowledges, skills and abilities required are intelligence and intelligence-related.

PHYSICAL SECURITY AND LAW ENFORCEMENT CAREER PROGRAM (CP-19):

The primary role of people in this career program is to provide physical security measures to protect the Army's assets against unauthorized access, damage, and theft; and to guard the Army's people and installations against criminal and terrorist acts.

The career program encompasses physical security, force protection, law enforcement, and criminal investigations.

Physical Security Specialists perform functions concerned with physical measures designed to prevent unauthorized access to equipment, installations, and material. Physical measures involve the total spectrum of procedures, facilities, equipment, and personnel employed to provide a secure environment for such assets.

Force Protection Specialists perform functions concerned with security programs designed to protect soldiers, civilian employees, family members, and equipment; in all locations and situations. The security programs are accomplished through planned and integrated application of combatting terrorism, physical security, operations security, personal protective services; and supported by intelligence, counterintelligence and other security programs.

Law Enforcement Specialists perform functions concerned with the enforcement of law and order on installations and activities. The functions are similar to those accomplished by most police agencies in the civilian community.

Criminal Investigators plan and conduct investigations relating to alleged or suspected violations of criminal laws. The duties involved in this function are similar to those performed by investigators in Federal investigative agencies and civilian police detectives.

DEFINITION OF PHYSICAL SECURITY

(excerpt from AR 190-13, applicable to CP-19)

"Physical Security

That part of the Army security system, based on threat analysis, concerned with procedures and physical measures designed to safeguard personnel, property, and operations; to prevent unauthorized access to equipment, facilities, materiel, and information; and to protect against espionage, terrorism, sabotage, damage, misuse,and theft. Operations security (OPSEC) and security targeted against traditional criminal activity are included.

a. Physical security procedures include, but are not limited to, the application of physical measures to reduce vulnerability to threat; integration of physical security into contingency, mobilization, and wartime plans; the testing of physical security procedures and measures during the exercise of these plans; the interface of installation OPSEC, crime prevention and physical security programs to protect against the traditional criminal; training of guards at sensitive or other storage sites in tactical defense against and response to attempted penetrations, and creating physical security awareness.

b. Physical security measures are physical systems, devices, personnel, animals, and procedures employed to protect security interest from possible threats and include, but are not limited to, security guards, military working dogs, lights and physical barriers, explosives and bomb detection equipment, protective vests and similar equipment, badging systems, electronic entry control systems and access control devices, security containers, locking devices, electronic intrusion detection systems (IDSs), standardized command, control and display subsystems; radio frequency (R/F) data links used for physical security, security lighting, delay devices and assessment and/or surveillance systems to include closed circuity television (CCTV). Depending on the circumstances of the particular situation, security specialists may have an interest in other items of equipment such as armored sedans. ... "

REGULATORY DEFINITIONS APPROPRIATE TO CP-19 GS-080, CP-35 GS-080 AND GS-132

The definitions listed below are references found in Army Regulations (AR) which govern the following:

GS-080 physical security work covered by CP-19 (non-CIPMS);

GS-080 security functional specialties which are intelligence-related covered by CIPMS CP-35; and,

GS-132 counterintelligence (CI) work covered by CIPMS CP-35.

The definitions are provided as guidance to distinguish between physical security, intelligence-related and intelligence work.

DEFINITIONS	AR REFERENCES	COVERED BY CAREER PROGRAM / SERIES CP-19 GS-080 / CP-35 GS-080 / GS-132
Counterintelligence: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations, conducted for or on behalf of foreign powers, organizations or persons, or terrorist activities, but not including personnel, physical, document, or communications security programs.	(AR 381-20 dated 26 September 1986)	X
Counterintelligence collection: The acquisition of information of a counterintelligence nature by means of direct observation, liaison with official agencies, or solicitation from other sources in response to officially approved counterintelligence collection requirements. Counterintelligence collection may be developed during investigations or operations, or may be acquired for the specific purpose of satisfying a requirement. Information will be considered as "collected" only when it has been made part of the files or information holdings of an Army intelligence component.	(AR 381-20 dated 26 September 1986)	X

DEFINITIONS	AR REFERENCES	COVERED BY CAREER PROGRAM / SERIES CP-19 GS-080 / CP-35 GS-080 / GS-132
Counterintelligence investigation: The systematic collection of information regarding a person or group, which is or may have engaged in espionage or other clandestine intelligence activity, sabotage, terrorist activities, or assassinations, conducted for or on behalf of, foreign powers, organizations or persons.	(AR 381-20 dated 26 September 1986)	X
Counterintelligence operations: Actions taken against hostile intelligence services to counter espionage and other clandestine intelligence activities damaging to national security.	(AR 381-20 dated 26 September 1986)	X
Counterintelligence production: The process of converting significant counterintelligence information into intelligence through the evaluation, analysis, integration and interpretation of all source data.	(AR 381-20 dated 26 September 1986)	X
Multidiscipline CI Analysis: Work involving the assessments of threats to U.S. security presented by activities of hostile intelligence collection systems. Includes all-source analysis of the integrated combined effort of hostile collection disciplines, and SIGINT, HUMINT, and IMINT, and special operations controlled by hostile intelligence agencies.	(AR 381-20 dated 26 September 1986)	X
Foreign Intelligence: Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons. Foreign intelligence does not include CI, except for information on international terrorist activities.	(AR 381-12 dated 1 July 1981)	X

DEFINITIONS	AR REFERENCES	COVERED BY CAREER PROGRAM / SERIES	
		CP-19 GS-080 / CP-35 GS-080 / GS-132	
Information Security: The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.	(AR 380-5 dated 25 February 1988)	X	
Information Systems Security: A composite of means to protect telecommunications systems and automated information systems and the information they process.	(AR 380-19 dated 1 August 1990)	X	
Intelligence: Information and related material describing U.S. foreign intelligence sources and methods, equipment, and methodology unique to the acquisition or exploitation of foreign intelligence, foreign military hardware obtained for exploitation, and photography or recordings resulting from U.S. foreign intelligence collection efforts. It may or may not include SCI.	(AR 380-10 draft dated 28 Aug 92)		X
Intelligence Activities: Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333, "United States Intelligence Activities," December 4, 1981.	(AR 381-10 dated 1 July 1984)		X
Intelligence-related: GS-080 intelligence-related work is work which involves the direction, planning, development, implementation, coordination, control, inspection, or conduct of specific programs. These programs are designed primarily to protect information, materiel, operations, and/or facilities from such national security threats as compromise, unauthorized disclosure, or espionage. The work typically involves one or more of the following security specialties: (a) Personnel, (b) Information, (c) Industrial, (d) Technology, (e) Foreign Disclosure, (f) Communications, (g) Electronics, (h) Operations, or (i) Automation.	(AR 690-13 dated 30 September 1990)	X	

DEFINITIONS	AR REFERENCES	COVERED BY CAREER PROGRAM / SERIES CP-19 GS-080 / CP-35 GS-080 / GS-132
Law Enforcement Activities: Activities undertaken for the purpose of detecting violations of law or to locate and apprehend persons who violate the law. This includes activities to enforce the Uniform Code of Military Justice. *(Some CP-35 GS-132 (CI) Special Agents are empowered with criminal investigative responsibilities limited to crimes involving national security such as espionage. CI Special Agents also are authorized by Executive Order 12333 to provide limited assistance to law enforcement authorities.)*	(AR 381-10 dated 1 August 1984)	X
Law Enforcement Duties: 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, and implementing related security controls. *(CP-19 GS-080s can be involved in the supervision of Guard and Police work.)*	(CIPMS AOG for GS-080 dated June 1991)	(Guard Series, GS-085, or Police Series, GS-083, depending on the specific duties and responsibilities.) X

DEFINITIONS	AR REFERENCES	COVERED BY CAREER PROGRAM / SERIES	
		CP-19 GS-080	CP-35 GS-080 / GS-132
Operations Security: A process of analyzing friendly actions attendant to military operations and other activities to -- a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.	(AR 530-1 dated 1 May 1991)	X	X
Personnel Security: The application of standards and criteria to determine whether or not an individual is eligible for access to classified information, qualified for assignment to or retention in sensitive duties, and suitable for acceptance and retention in the total Army consistent with national security interests.	(AR 380-67 dated 9 September 1988)		X
Physical Security: That part of security concerned with physical measures designed to safeguard personnel, to prevent or delay unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage and theft. *(CP-35 GS-080s do physical security work primarily in relation to the security of sensitive or classified military information.)*	(AR 190-13 to be published in UPDATE 3)	X	

DEFINITIONS	AR REFERENCES	COVERED BY CAREER PROGRAM / SERIES CP-19 GS-080 / CP-35 GS-080 / GS-132
Security Countermeasures: Those efforts undertaken to protect the national security against foreign intelligence threats by safeguarding classified and sensitive information (Information Security), personnel with access to such information (Personnel Security) and defense industry organizations with access to such information (Industrial Security). *(Functional security specialties specified in the GS-080 AOG align with the above categories as follows: Information Security can include Information, Disclosure, Physical and Operations specialties; Information Systems Security can include Automation and Technical specialties; Personnel Security includes the Personnel specialty; and, Industrial Security includes the Industrial specialty.)*	(Based on DA DCSINT functional definition, March, 1993)	X
Sensitive Compartmented Information (SCI): All information and materials requiring special community controls indicating restricted handling within present and future community intelligence collection programs and their end products. These special community controls are formal systems of restricted access established to protect the sensitive aspects of sources, methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.	(Confidential AR 380-28, Department of the Army Special Security System (U) dated 1 September 1991)	X
Sensitive Information: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy of individuals, but which has not been specifically authorized under an Executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy (PL 100-235, 8 Jan 88).	(AR 530-1 dated 1 May 1991)	X

DEFINITIONS	AR REFERENCES	COVERED BY CAREER PROGRAM / SERIES CP-19 GS-080 / CP-35 GS-080 / GS-132
Special Access Program: A sensitive activity approved specifically by the Secretary of the Army imposing a "need to know" or access controls beyond those normally required for access to CONFIDENTIAL, SECRET, or TOP SECRET information. Such controls include, but are not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine "need-to-know"; or special lists of persons determined to have a "need-to-know.	(Confidential AR 380-381, Special Access Programs(U))	X

CLARIFYING GUIDANCE - QUESTIONS AND ANSWERS

The following questions and answers are designed to resolve definitional problems and clarify differences in work among CP-19 GS-080, CIPMS GS-080, and GS-132. They clarify the difference between Security Countermeasures, Counterintelligence and other functional areas of GS-080 work (where similar functions are found under both CP-19 and CP-35), and they explain the difference between intelligence-related versus intelligence work.

1. What is the major difference between security administration work covered by CIPMS GS-080 and security work that is non-CIPMS covered in CP-19?

CIPMS GS-080 work is primarily concerned with protection against foreign intelligence threats. Non-CIPMS work is primarily concerned with protection against other criminal threats (both foreign and domestic).

The major difference between CIPMS and non-CIPMS security work is that CIPMS work is intelligence-related. The determination that security work is intelligence-related is based on the source of the guidance being implemented and the proponent of that guidance. In the Army, the DCSINT is the proponent of 380 and 381 series regulations. Therefore, the determination was made that GS-080s who devote more than 50% of their time in support of those regulations were intelligence-related and should be in CIPMS.

2. What is the difference between intelligence versus intelligence-related work?

Intelligence work consists of functions directly associated with the foreign intelligence process (e.g., the acquisition of information on foreign activities, the analysis of that information and the production of foreign intelligence). Intelligence-related work can be functions in support of these activities or similar work that are **not** formally a part of the foreign intelligence process. In the Army, "intelligence related" can also be used to distinguish between CP-35 and CP-19 GS-080 work in that CP-35 is a part of the intelligence community and CP-19 is not.

3. Can CIPMS GS-080 work in CP-35 and non-CIPMS GS-080 in CP-19 be mixed in the same position? Is this a good idea? What might be some problems when this is done?

The two types of work can be mixed in the same position. It is neither a good nor bad idea, merely a fact of life at many locations where there are only one or two GS-080s. Application of the "at least 51%" rule should minimize any problems associated with "mixed" positions.

4. Must a GS-080 position deal with classified material, per se, in order to be considered covered by CIPMS?

This is not a good criterion to determine CIPMS coverage. However, it is conceivable that a CIPMS position would not deal with classified information, but it would certainly be the exception. Most CIPMS positions have a clearability condition of employment.

In CIPMS, a GS-080 position must include a predominance (at least 51%) of intelligence-related duties involving the direction, planning, development, implementation, coordination, control, inspection, or conduct of specific programs. Such programs are designed to protect information, material and operations.

5. Is it likely that a position would include the following mix of work: CIPMS GS-080, non-CIPMS GS-080, and GS-132 (e.g., Case Officer (CI) or Investigator (CI)?

No. GS-080s in Army MACOMs and at installations may perform a mix of CIPMS and non-CIPMS work (and most of the more senior positions should) but none of these positions would require investigative or case officer work. GS-132 case officers and investigators may require familiarity with GS-080 work but do not perform this work.

6. What are examples of "systems" that might be developed, evaluated, maintained or operated to safeguard information (from CIPMS GS-080 series definition). Are these systems different from those applied by non-CIPMS Physical Security Specialists under CP-19?

The best examples of security systems to safeguard information are Communications Security (COMSEC), personnel security, document security and ADP security systems, or aggregates of these. These are different from such physical security systems as guard forces, intrusion detection systems and other forms of physical barriers. The key difference is that physical security systems almost always can be used to help secure information but information security systems can rarely be used to provide physical security. Physical security systems are, as their name

implies, **physical**. They can be seen and touched and they are usually associated with or fixed in one place. Information security systems are more generally **understood** than seen or touched and they do not have to be associated with or fixed in one place. They can be world wide in scope.

7. What is the best way to tell the difference between non-CIPMS CP-19 and CIPMS CP-35 080 work when the series definitions between the OPM GS-080 classification standard and the Army CIPMS AOG for GS-080 are so similar?

CIPMS CP-35 GS-080 work is primarily associated with protecting against foreign intelligence threats. Non-CIPMS CP-19 GS-080 work is primarily associated with protecting against all other threats. See also answer to question 1. The key is the term "intelligence-related".

8. What is the difference between CIPMS GS-080 work and CP-19 Provost Marshal work when both are required for example to "protect ... information... facilities... from national security threats?"

It all relates back to what is intelligence-related and the decision that the regulations and procedures being implemented are a primary determinant of what is or is not intelligence related. As such, the people who implement 380 and 381 series regulations to "protect...from...threats" are doing CIPMS things while the individuals who implement 190 series regulations for the same purpose are CP-19.

9. What does the title "security manager" really mean in the context of the GS-080 profession?

The term Security Manager pertains exclusively to information security duties. Chapter XIII, AR 380-5, paragraph 13-304 requires appointment of security managers at each DoD activity and lists a whole range of duties the security manager is to perform. A grade requirement is included.

10. What does the title "security officer" really mean in the context of the GS-080 profession?

Different things to different people. The preferred interpretation is as defined in the AOG for GS-080 Security Administration. The Security Officer is the individual who handles the overall development and installation management of security programs.

11. Elaborate on what "managing a multi-functional activity security program..." means (from CIPMS GS-080 series definition).

Multi-functional is meant to describe security, not activity. That is, an activity which requires a multi-functional security program with a security manager who is responsible for more than one security function--a security function being each of the specialties identified in the AOG: information, personnel, disclosure, etc.

12. By definition, both intelligence-related and non-intelligence related GS-080 security specialists protect personnel, property and operations. What is the difference between CIPMS GS-080 work and non-CIPMS GS-080 work within these responsibilities.

See discussion in question 8. It all relates back to policies the specialist implements, the proponent of those policies, and, in some cases, the organization for which the work is performed.

13. What does security countermeasures mean in the context of CIPMS GS-132 (CI) work?

Many CI specialists provide advice and guidance to security countermeasures (GS-080) specialists. For example, CI agents conduct a variety of services in support of Special Access Programs (SAPs) to help SAP security managers do their jobs better. CI agents routinely provide assistance to installation security managers concerning ways to counter the foreign intelligence threat. These types of support are analogous to a police officer advising a bank security manager on how to better secure the bank or to a fire fighter advising a school fire marshall on how to better fire-proof the school.

14. What does counterintelligence mean in the context of CIPMS GS-080 work?

This is the logical inverse of the previous question. GS-080 security specialists are dependent on counterintelligence specialists for information concerning how to counter foreign intelligence threats.

15. What does counterintelligence mean in the context of CIPMS GS-080 work and GS-132 (CI)?

Counterintelligence refers to activities (operations, investigations, collection, analysis and production) to understand and counter specific foreign intelligence threats.

16. (p 10, GS-080 AOG) What is the difference between CP-19 and CP-35 GS-080 work in reference to the protection of information, processes and equipment in the automated systems environment ... from physical or electronic unauthorized disclosure or physical destruction? Are they not both involved with physical security?

They are both involved with physical security but CP-19 work is involved almost **entirely** with physical security while CP-35 work is more involved with security processes to protect against foreign intelligence threats. CP-19 work is more concerned with protection against physical destruction and deals very little if at all with electronic unauthorized disclosure. CP-35 work is less involved with protection against physical destruction and more involved with protection against electronic unauthorized disclosure.

17. (p.2, Section A, GS-132 OPERATIONS AOG) What is the difference between the counterintelligence and security activities performed by GS-132 Intelligence Specialists and that performed by GS-080 Security Specialists?

Counterintelligence and security activities performed by GS-132 Intelligence Specialists are operations, investigations, collection, analysis and production associated with specific foreign intelligence threats. GS-080 Security Specialists are performing work generally associated with the application of security countermeasures against a broad range of foreign intelligence threats.

18. (p.2, Section A, GS-132 OPERATIONS AOG) What type of security knowledges must the intelligence specialist know to perform intelligence operations? How is this security work different from GS-080 security specialist work? What is the best explanation that the predominate knowledge in these positions fall within the GS-132 series?

An intelligence specialist should be familiar with the broad range of security countermeasures to protect his or her activities from foreign intelligence exploitation. This is **not** security work. It is not endemic to intelligence operations. **All** Army employees who deal with sensitive information must have these knowledges. Just as the practice of good safety is not "safety work," this is not "security work." Work that involves intelligence operations, investigations, collection, analysis or production provides the best evidence that a position falls within the GS-132 series.

19. (p.2, GS-080 AOG) Since some security positions require knowledge of basic intelligence program functions and requirements, what is the best evidence that the predominate knowledge of such positions is within the CIPMS GS-080 series?

Work that involves the application of security countermeasures techniques, systems or procedures provides the best evidence that a position falls within the GS-080 series. Knowledge of basic intelligence program functions can be helpful but need not be central to GS-080 positions.

20. (p.3, Section A, GS-132 OPERATIONS AOG) How is the intelligence operations discipline of Counterintelligence (CI) different from the counterintelligence performed by GS-080 security specialists? If both series cover counterintelligence, what is the best evidence that a position falls within the GS-080 or GS-132 series?

Counterintelligence operations, investigations, collection, analysis or production should not be performed by GS-080 security specialists. The GS-132 practitioner normally investigates, analyzes and produces CI threat data. The GS-080 practitioner evaluates and applies that data to the security system design.

21. (p.16, GS-080 AOG) What is the difference between the physical security performed by CIPMS Security Specialist (Physical) and the physical security performed by CP-19 GS-080?

CIPMS physical security work is generated by regulations falling under the CIPMS umbrella. For example, many regulations in the 380 series require physical security KSAs - safeguarding standards for classified information and material; protection, inspection, and inventory requirements for COMSEC material; physical security standards for SAP or Sensitive Compartmented Information Facilities; physical security of automated information systems. The physical security work performed by CP-19 personnel is accomplished pursuant to 190 series regulations, e.g., security of arms, ammunition, and explosives; protection of restricted areas; movement control; protection of sensitive items; etc.

22. (p.6, Section A, GS-132 OPERATIONS AOG) How is Investigator (CI) work which is described as: "Conducts and/or oversees investigations concerned with alleged or suspected offenses against the laws of the United States, determining compliance with laws and regulations, or individual suitability for access to classified national security information. These include the following types of investigations: personnel security, deliberate security violations, subversion and espionage, technical surveillance, and polygraph examination." different from CIPMS GS-080 work?

CIPMS GS-080 work should not involve formal CI investigative work. GS-080 investigative functions, generally, are limited to preliminary fact-finding inquiries. Formal CI investigations are conducted by GS-132s.

23. (p.17, GS-080 AOG) Is the function of security countermeasures mainly covered under the description of Security Specialist (Technical)? This functional specialty includes the security subfunctions of communications security (COMSEC), electronics security (ELSEC), TSCM (technical surveillance countermeasures) and TEMPEST (compromising emanations).

No. These are technical subfunctions and do not include other significant security countermeasures functions such as personnel security, information security and industrial security.