

POSITION DESCRIPTION (Please Read Instructions on the Back)

1. Agency Position No.
NL12395

2. Reason for Submission <input checked="" type="checkbox"/> Redescription <input type="checkbox"/> Reestablishment Now <input type="checkbox"/> Other	3. Service <input type="checkbox"/> Hdqtrs. <input checked="" type="checkbox"/> Field	4. Employing Office Location Orlando, FL.	5. Duty Station	6. OPM Certification No.
7. Fair Labor Standards Act <input checked="" type="checkbox"/> Exempt <input type="checkbox"/> Nonexempt		8. Financial Statements Required <input checked="" type="checkbox"/> Executive Personnel Financial Disclosure <input type="checkbox"/> Employment and Financial Interests		9. Subject to IA Action <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
10. Position Status <input checked="" type="checkbox"/> Competitive <input type="checkbox"/> Excepted (Specify in Remarks) SES (Gen.) <input type="checkbox"/> SES (CR)		11. Position is: <input type="checkbox"/> Supervisory <input type="checkbox"/> Managerial <input checked="" type="checkbox"/> Neither	12. Sensitivity 1 - Non-Sensitive <input type="checkbox"/> 2 - Noncritical Sensitive <input type="checkbox"/> 3 - Critical Sensitive <input checked="" type="checkbox"/> 4 - Special Sensitive <input type="checkbox"/>	
Explanation (Show any positions replaced) Replaces: NL10599		13. Competitive Level Code 1196		
14. Agency Use				

15. Classified/Graded by	Official Title of Position	Pay Plan	Occupational Code	Grade	Initials	Date
a. U.S. Office of Personnel Management						
b. Department, Agency or Establishment						
c. Second Level Review						
d. First Level Review	Security Officer	GS	0080	12		
e. Recommended by Supervisor or Initiating Office						

16. Organizational Title of Position (if different from official title) _____
17. Name of Employee (if vacant, specify) _____

18. Department, Agency, or Establishment Department of the Army	c. Third Subdivision Chief of Staff (CS)
a. First Subdivision U.S. Army Materiel Command (AMC)	d. Fourth Subdivision Administrative Operations Division (CSA)
b. Second Subdivision Simulation, Training and Instrumentation Command (STRICOM)	e. Fifth Subdivision

19. Employee review - This is an accurate description of the major duties and responsibilities of my position. _____
Signature of Employee (optional) _____

20. **Supervisory Certification.** I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out Government functions for which I am responsible. This certification is made with the knowledge that this information is to be used for statutory purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.

a. Typed Name and Title of Immediate Supervisor William C. Youmans, Acting Staff Operations Officer	b. Typed Name and Title of Higher-Level Supervisor or Manager (optional)
Signature _____ Date 8/27/01	Signature _____ Date _____

21. **Classification/Job Grading Certification.** I certify that this position has been classified/graded as required by Title 5, U.S. Code, in conformance with standards published by the U.S. Office of Personnel Management or, if no published standards apply directly, consistently with the most applicable published standards.
22. Position Classification Standards Used in Classifying/Grading Position
USOPMPCS Security Administration Series, GS-0080, Dec 1987, TS-82, Jul 99, HRC-7; USOPM Digest of Significant Classification Decisions and Opinions, No. 7, Aug 85.

Typed Name and Title of Official Taking Action
James L. Laughlin, Colonel, GS, Chief of Staff

Signature _____ Date 4 Sep 01

Information for Employees. The standards, and information on their application, are available in the personnel office. The classification of the position may be reviewed and corrected by the agency or the U.S. Office of Personnel Management. Information on classification/job grading appeals, and complaints on exemption from FLSA, is available from the personnel office or the U.S. Office of Personnel Management.

23. Position Review	Initials	Date								
a. Employee (optional)										
b. Supervisor										
c. Classifier										

24. Remarks
Position is at the Full Performance Level.
BUS: 7777

INTRODUCTION

This position is in the Office of the Chief of Staff within the Simulation, Training and Instrumentation Command (STRICOM), a major subordinate command for the U.S. Army Materiel Command (AMC). The mission of STRICOM is to provide centralized management and direction for all research, development, acquisition and fielding of Army training devices, simulations and simulators, instrumentation, targets and threat simulation. The commander centrally directs, coordinates, and supports the materiel development, acquisition and sustainment activities through the matrix organization and four Project Managers. STRICOM programs have high profile due to the complex nature of the simulation technology and the emphasis on training to meet the Chief of Staff of the Army's vision. Incumbent serves as Command Security Officer responsible for Physical, Personnel, Information, Industrial, Disclosure, Operations, Force Protection and Technology Security functions. Serves as the Command Security Manager, OPSEC Officer, Physical Security Officer/Provost Marshal, Foreign Disclosure Officer, Technology Protection Officer, and Force Protection Program Manager; designated positions required by Army Regulations. Serves as principal advisor to the Commanding General, Command Group, Program Managers (PMs) and Directors on all security matters.

MAJOR DUTIES

1. Manages the Command Information Security Program with direct responsibility to the Commanding General, Deputy to the Commander, Chief of Staff, Directors and Program Managers. Interprets regulatory requirements and establishes the criteria for protecting Classified Military Information (CMI) and Controlled Unclassified Information (CUI) within the command. Provides security classification guidance for classification of documents generated by the command to include the publication of Security Classification Guides for STRICOM products in support of classified programs. Provides staff supervision over personnel performing Information Security functions. Responsibility for the STRICOM Inventory, Control and Accountability program which tracks all classified documents and/or material. Investigates security violations and determines course of action and damage assessment. Initiates investigations as required by DoD regulations for those incidents involving probable or confirmed compromise consisting of a two-stage approach: (1) interviews personnel that are involved, coordination with local Defense Criminal Investigative Service (DCIS) and Defense Security Service (DSS) agents as appropriate; (2) provides preliminary reports to higher echelons of command and the proponent commands with follow-ups as events develop with recommendations for courses of action to be taken, alternates, etc. Notifies and coordinates with originators of classified information on

compromised or suspected compromises of classified information, to include higher echelons in the DoD, DA, AMC and at times, various contractors. Destroys classified materials in conformance with existing regulations that states how and under what conditions the material at each level will be destroyed.

10%

2. Manages the Command Personnel Security program with responsibility for all facets of the personnel clearance program. Interprets regulatory requirements and establishes the criteria for position sensitivity levels and personnel security investigative requirements to access Classified Military Information (CMI) by DoD and Support Service Contractor personnel within the Command. Ensures that all STRICOM employees and contractors that are required to perform their duties using classified materials and/or documents, are granted access based on proper documentation from the necessary investigative and adjudication agency. Maintains the Top Secret, Sensitive Compartmented Information (SCI), NATO Access and Special Access Program (SAP) Billet Control Systems. Sponsors contractors or consultants for security clearances in those cases that an individual is in fact acting as a consultant. Ensures that all STRICOM and contractor personnel that require access to the STRICOM information network have undergone the proper level of background security investigation appropriate for the information technology level they are working at and grants the appropriate security access. Conducts required orientation briefings for new employees that cover all phases of security except Information Systems security. Informs all new employees of the basic security requirements with appropriate references to include the process for an employee to obtain a clearance in fulfillment of assignments. Schedules and conducts the annual employee multidiscipline security briefing(s) as part of the overall security education program required by current Army security program regulations. Oversees personnel performing Personnel Security functions. Serves as the primary point of contact between STRICOM and Defense Security Service, Defense Industrial Security Office, Office of Personnel Management and the military central clearance offices on Personnel Security matters.

15%

3. Manages the National, DoD and Army Industrial Security Program for the command. Reviews all classified procurement initiated by STRICOM with private contractors requiring access to or generation of classified information. Provides Security Classification guidance (DD Form 254) for these contracts and monitors these to validate that they are still required and

are up to date. Provides guidance, maintains and monitors the DD Form 254 (Contract Security Classification Specification) for all classified contracts. Maintains contact with offices of the Defense Security Service Industrial Security Office and the 902d Military Intelligence Group to ensure facility clearances are current and meet requirements levied by DoD instructions for the protection and storage of classified materials at contractor facilities. Advises the Commander, Directors and Project Managers on Industrial Security matters.

15%

4. Serves as the Physical Security Officer and MSC Provost Marshall for the Command. Prepares and implements the STRICOM personnel and property security program. Advises the command on physical security risks and on the best action to take. Identifies and designates those areas that are Restricted Areas and Mission Essential Vulnerability Areas (MEVA). Interfaces with the Host Command Security Police Office to ensure that adequate physical security measures are in place in support of STRICOM. Coordinates with the Host Command Security Police Office for Law Enforcement, Crime Prevention and Security Inspection support to the Command. Coordinates with local offices of the FBI and local law enforcement to determine the criminal threat to STRICOM personnel and property. Coordinates and gains approval to issue all special category badges (i.e., foreign national, unescorted contractor, student, and contractor badges) which encompasses both employees and incoming DoD and contractor employees. Coordinates and manages the outgoing visit request program for employees, ensuring proper format, certification data and origination of visit request is in consonance with existing directives. Participates in unannounced security inspections which are directed to ensure that STRICOM maintains their "security envelope" as established in appropriate DoD, DA, AMC guidelines/regulations.

10%

5. Serves as the Foreign Disclosure Officer for the Command. Reviews and provides final approval for the release/disclosure of both classified and unclassified technology information to foreign sources. Secures the necessary approval from various levels of government prior to the release/disclosure of any classified information to a foreign government or contractor. Interfaces with DoD, Defense Intelligence Agency (DIA), DA, AMC etc. Manages the National, DoD and Army policy on disclosure of information and technology transfer to Foreign Representatives and non-government activities. Provides foreign disclosure and counter-intelligence support to the International Programs, Foreign Military Sales and Munitions Case Licensing decisions. Reviews all Delegation of

Disclosure Letters (DDL), Drug Enforcement Administration (DEA), Public Affairs (PA), and Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) documents for completeness. Investigates any unsolicited requests for information that are questionable to determine if the request has foreign disclosure or counterintelligence concerns. Operates the Foreign Disclosure and Technical System (FORDTIS) and Foreign Visits program for the Command. Provides threat briefings and debriefings to STRICOM personnel meeting with Foreign Representatives or attending International meetings. Implements the Subversion and Espionage Directed against the Army (SAEDA) program within STRICOM.

15%

6. Serves as the Technology Protection Officer for the Command. Implements and manages the Technology Protection Program to ensure the protection of unclassified but sensitive critical technology and controlled unclassified information (CUI). Interprets the various DoD, DA and AMC regulations, International Traffic in Arms Regulations (ITARs), Exchange Agreement Regulations (EARs), and Military Critical Technologies Lists (MCTLs) as they apply to the STRICOM mission. Provides guidance to the Commander, Directors and PMs on identifying Critical Program Information (CPI) and establishing Acquisition Program Protection Plans, Technology Assessment/Control Plans (TA/CP), and Classified Information (CI) Support Plans. Oversees STRICOM classified meetings in support of mission objectives. Incumbent is responsible for ensuring the area to be used is properly evaluated, all participants, including contractors, have clearance documentation/certification at the required level. Coordinates all dissemination of classified data/information, controls access to such briefings, and ensures that proper storage facilities are available at the termination of such briefings/meetings, whether during breaks or overnight.

10%

7. Prepares and implements the Command Force Protection Program by serving as the Force Protection Program Manager for the Command. Performs risk assessments of STRICOM facilities to determine what cost-effective protective measures are appropriate to counter the risk. Collects and maintains information concerning the foreign and domestic terrorist threat to STRICOM personnel and facilities. Coordinates with the local FBI, law enforcement, and 902d Military Intelligence (MI) Group offices to determine the local terrorist threat and contacts the Defense Intelligence Agency (DIA), DA and the US Forces Commander-in-Chiefs (CINCs) for the latest international terrorist threat. Collects terrorist threat data from the various open source and foreign force protection

sources. Provides travel threat briefings on the terrorist and intelligence threat to all STRICOM personnel who perform OCONUS official travel and to those traveling for pleasure who so desire it. Advises the Command on changes in threat and provides information on personal and travel security to all STRICOM personnel. Oversees the security portions of the STRICOM Foreign Travel program and the interpretation of applicable policies and regulations requiring contact with the DoD Passport Office and State Department. Maintains awareness of all travel restrictions, passport and visa requirements and ensures that those employees traveling are properly briefed and upon return, conduct an appropriate debriefing. Authenticates the requirement for "no fee" passports and visas and ensures the applications are complete. Authorizes the use of "tourist" passports for official travel when the threat situation dictates.

15%

8. Prepares and implements the Command OPSEC Program by serving as the Operations Security (OPSEC) Officer for the Command. Ensures that OPSEC measures are implemented in all programs that deal with classified or technology sensitive issues. Reviews each individual technical report, document, briefing, etc. to ensure that critical military technology or those products covered by the export laws are not released to the public. Tracks products covered by the export laws throughout STRICOM, takes follow-up actions and extensive coordination at times of short deadlines. Reviews and approves all submissions to the STRICOM Web Page for OPSEC considerations prior to their release. Collects, maintains, and advises the Commander, Directors, and PMs on information concerning the foreign intelligence threat to STRICOM programs.

10%

Performs other duties as assigned.

FACTOR 1 - KNOWLEDGE REQUIRED - LEVEL 1-7 - 1250 Points

The incumbent is considered the major authoritative source for multi-functional security program knowledge for STRICOM using:

- Extensive, in-depth knowledge of a wide range of multi-functional security concepts, principles and practices to review, analyze and resolve complex security problems.
- Comprehensive knowledge of new security requirements established in legislation, regulations, and various policy statements as related to the protection of classified material

and controlled unclassified material that will effect the various STRICOM security programs.

- Knowledge and understanding of Information Technology (IT) operating systems, network concepts and operations, and techniques related to the Information Security (IS) program and any other interfacing security program (i.e., physical, industrial, etc.) to develop and/or recommend enhancements to improve systems security for a wide variety of users.
- Knowledge and understanding of the functions, organizational components, and products of STRICOM and their relationship with other government and DOD agencies and industrial organizations.
- Knowledge of the federal, DOD, Combat Commands, DA organization and specific function of each to identify the appropriate agency to contact for coordination functions.
- Knowledge and experience in the handling, control, inventory, accountability, marking and destruction of classified material(s) and/or equipment; classification authority and established guidelines.

FACTOR 2 - SUPERVISORY CONTROLS - LEVEL 2-4 - 450 Points

Incumbent's immediate supervisor, the Staff Operations Officer, provides very broad and general programmatic guidance. Responsibility is given in terms of objectives and priorities expected of the programs. Incumbent receives technical supervision from the Senior Intelligence Officer or other security personnel at higher headquarters with extremely complex situations that have no precedent. The incumbent often receives direct tasking from AMC Staff elements and other DA and DOD agencies that are usually acted upon directly.

Incumbent is relied upon to independently exercise sound judgment and initiative in developing, recommending and implementing procedures which will result in effective and efficient Physical, Personnel, Information, Industrial, Disclosure, Operations and Technology Programs. Incumbent is also relied upon to provide advice and recommendations, which may serve as a basis for policy decisions with respect to the security program at STRICOM. Incumbent often renders technical judgements and decisions on program matters during meetings, conferences, inspections and consultations. The supervisor is kept informed of significant developments.

Performance is reviewed in terms of maturity of judgement in resolving problems and soundness of recommendations on new policies or their interpretation. Recommendations for new

projects and shifts in security program objectives are evaluated in terms of resources available, program goals, or DA-wide priorities. Completed work is reviewed from an overall standpoint in terms of feasibility and effectiveness in meeting objectives and achieving expected results.

FACTOR 3 - GUIDELINES - LEVEL 3-4 - 450 Points

Guidelines regularly used in the work are in Public Law, Executive Orders, DoD, Army and AMC Directives. Security programs are governed by multiple DoD/DA regulations/policies. Policies and procedures available are generally stated in broad terminology and not always applicable to specific situations. Guidelines for the identification of intelligence, counterintelligence and the engineering and analyses efforts requiring technical protection must be derived through discussions with program managers and technical personnel.

Incumbent must use initiative, resourcefulness, sound judgment and discretion with broad latitude, to: interpret the intent of guidelines and apply across the organization; develop improved methods and more specific procedures that allow conformance with DOD/DA instructions and/or policies, and; ensures the protection of each program from inadvertent disclosure. Considerable judgment is required in security suitability determinations in applying security community policy to access sensitive material.

FACTOR 4 - COMPLEXITY - LEVEL 4-5 - 325 Points

Incumbent serves as the resident technical expert for Physical, Personnel, Information, Industrial, Disclosure, Operations, and Technology Security programs and functions. Incumbent is responsible for identifying and evaluating trends in security violations, other lapses in security; and in measuring organizational effectiveness in achieving overall STRICOM security objectives and goals.

The decision on what needs to be done depends upon multiple factors, which must be analyzed and prioritized according to overall effect upon the command. The work involves different and unrelated processes and methods. Incumbent typically assesses situations complicated by conflicting and/or insufficient data which must be analyzed to determine the applicability of established methods, the need to digress from these methods and techniques or whether specific kind of waivers can be justified. Consideration must be given to probable areas of future change in systems designs, equipment development or comparable aspects of projects in order to facilitate subsequent modifications as to contractual documentation including the DD Form 254. In these assessments relative to weapons technology, incumbent must weigh voluminous materials determining classification foreign

disclosure permitted export law/lists, etc. A myriad of policies, regulations and guidance must be reviewed, interpreted, and applied. This effort involves problem definition and resolution, recommendation and implementation of various changes in policies and regulations that govern the scientific and non-scientific endeavors of the command.

The range of programs, scientific disciplines, sources of information, volume of information processes, and inter-service coordination contribute to the complexity of this assignment. Constantly changing technology add to the complexity since each new program does not routinely follow the pattern of an existing program. The implementation of command security policies, practices, procedures and techniques have to be varied for a number of environments/locations that differ in kind and level of security requirements and the local conditions requiring adjustment in established approaches or documented guidelines. Incumbent provides direct support to Tenant activities and their unique requirements in the security arena.

FACTOR 5 - SCOPE AND EFFECT - LEVEL 5-3 - 150 Points

The purpose of the work typically involves resolving a variety of conventional security problems, questions and situations such as those where responsibility has been assigned for monitoring established security systems and programs and performing independent reviews and recommending actions involving well-established security criteria, methods, techniques, and procedures. However, incumbent does develop supplemental security procedures, guidelines, etc., for an ever-changing multi-functional environment.

Incumbent's work products, advice, and assistance effects the effectiveness and efficiency of ongoing security programs and contributes to security effectiveness of newly introduced programs and facilities requiring such protective services. The effect of the work is primarily local in nature, however, incumbent's work also effects STRICOM contractor facilities located throughout U.S due to interlocking security requirements.

FACTOR 6 - PERSONAL CONTACTS - LEVEL 6-3 - 60 Points

This position requires personal, electronic mail, regular correspondence and telephonic contacts with individuals outside the Army, to include all echelons of government, DoD, civilian industry, scientific groups, foreign government personnel, state and local law enforcement officials and organizations, in pursuit of overall security program objectives. Contacts occur at both formal and informal briefings, workshops, and conferences, etc. Contacts take place in a moderately unstructured setting, i.e., 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.

FACTOR 7 - PURPOSE OF CONTACTS - 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. Persuasion and negotiation are necessary due to the presence of conflicting security, budgetary, and program objectives that must be resolved. Contacts with the Commander, directors, program managers, procurement personnel and contractors in an advisory relationship, is for the purpose of discussing policy matters, program plans or changes in program emphasis so that security systems may be applied to greater advantage.

FACTOR 8 - PHYSICAL DEMANDS - LEVEL 8-1 - 5 Points

The work is sedentary and is usually accomplished while the employee is comfortably seated at a desk or table. However, some walking, climbing and bending is required to inspect security facilities. Items carried typically are light objects such as briefcases, notebooks, and data processing reports. Lifting of moderately heavy objects is not normally required, although lifting of boxes containing documents may be required. No special physical effort or ability is required to perform the work.

FACTOR 9 - WORK ENVIRONMENT - LEVEL 9-1 - 5 Points

Work is primarily performed in an office-like setting or in a security vault involving everyday risks or discomforts which require normal safety precautions typical of such places as offices, meeting and training rooms. The work area is adequately lighted, heated and ventilated. Makes field trips to review overall security program and for the purpose of disseminating new technology and methods for STRICOM use.

Incumbent must be able to obtain and maintain a top secret clearance. Subject to drug testing IAW regulatory guidance.

NON-CRITICAL ACQUISITION POSITION AMENDMENT TO PD# NL 12395

"The employee must meet DoD 5000.52-M requirements applicable to the duties of the position."