District of Columbia National Guard
Accelerated Hiring Announcement
Title 5 Civilian
DC-AHA-AR-26-005

APPLICATION MUST BE FORWARDED TO: IN ORDER TO RECEIVE CONSIDERATION Mr. Rodriguez Cristian cristian.rodriguez20.civ@army.mil	**OPENING DATE:** 03 March 2026	**CLOSING DATE:** 06 March 2026
	Position Title: SUPERVISORY IT SPECIALIST (PLCYPLN) **Title** 5 Civilian **Grade:** GS-2210-13	
	AREA OF CONSIDERATION: All groups of Federal re-employables and eligibles.	
Position Location: JFHQ CIO/G6, DC ARMORY	**NOTE:** This position is subject to provisions of the DoD Priority Placement Program.	

INSTRUCTIONS FOR APPLYING:

You must send applications electronically to the email addresses listed below.

REQUIRED DOCUMENTS:

1. Resume - resume highlighting your specialized experience. Ensure you include "from (mm/yy)" and "to (mm/yy)" dates along with a description of your relevant experience. Note: starting on September 27, 2025, federal agencies will only accept resumes up to two pages in length.
2. Current SF-50 (If applicable)
3. Please submit completed packages to:
   Mr. Rodriguez Cristian
   cristian.rodriguez20.civ@army.mil

GENERAL EXPERIENCE:

Experience, education, and/or training that has provided a basic knowledge of data processing functions and general management principles that enabled the applicant to understand the stages required to automate a work process. Experience may have been gained in work such as computer operator or assistant, computer sales representative, program analyst, or other positions that required the use or adaptation of computer programs and systems.

SPECIALIZED EXPERIENCE:

1-year specialized experience equivalent to at least the next lower grade. Experience that demonstrated accomplishment of computer project assignments that required a wide range of knowledge of computer requirements and techniques pertinent to the position to be filled. This knowledge is generally demonstrated by assignments where the applicant analyzed a number of alternative approaches in the process of advising management concerning major aspects of ADP system design, such as what system interrelationships must be considered, or what operating mode, system software, and/or equipment configuration is most appropriate for a given project. Experience in managing the function of the work to be performed. Experience which includes leading, directing and assigning work of personnel.

Announcement Number: DC-AHA-AR-26-005

Position: SUPERVISORY IT SPECIALIST (PLCYPLN)

POSITION DESCRIPTION:

1. Manages IT activities for the DODIN-A(NG) and Mission Support Systems. Manages IT activities to ensure the appropriateness of system design, development, deployment, and security functions associated with the infrastructure and support systems, IT network and the inventory of software and hardware. Oversees the IT procurement process and administers an IT inventory management and replenishment program to ensure efficient life-cycle management. Provides Information System Cost Estimates for the support of Military Construction (MILCON) execution. This includes the construction and review of various management reports and processes used to define, value and tracks IT investments.

Manage the programs and priorities. Defines goals, objectives, plans, and performance measures for the IT services that are provided from the Department of Defense, Departments of the Army and Air Force, National Guard Bureau and other guidance while interpreting the guidance to ensure the State's IT activities are aligned with and support these objectives and goals. Coordinates implementation of the State's IT systems and strategic plans for integration into the Department of Defense, Departments of the Army and Air Force and National Guard Bureau priorities.

Reviews major IT investments for consistency with strategies, plans, and enterprise architectures through the MDEP Program Manager and the vision for the state. May serve as PM where appropriate initiating IT investments, including the need to implement a system of independently verifiable measures for cost, timeliness, quality, and system capability in meeting specified programmatic requirements. Performs cost-benefit analysis for all proposed IT procurements and is instrumental in decision-making to support funding for new initiatives.

Oversees the Mission Command (MC) Branch on all matters pertaining to MC and communication system readiness. Supervises support services (COMSEC, Spectrum Management, Radio, other MC systems, etc.) as well as emergency communication support actions supporting Domestic Operations (DOMOPS). Supervises overall support for MC systems for MTOE and TDA elements. Serves as alternate career manager for Signal/Cyber/Communication personnel in coordination with the Air and Army leadership. Additionally, establishes priorities of effort in support unit communication and MC support. Reports status on mission command systems and provides recommendations for support through parent Program Executive Offices/Program Management channels (PM WIN-T, CECOM, etc.). Manages, tracks, and reports career needs of Signal and Cyber personnel and makes recommendations on assignments. Maintain effective rapport with subordinate unit G6/S6 personnel, and agency representatives, ensuring unified efforts in communication support. Attends readiness briefings, Unit Status Reporting briefs and other meetings to ensure synchronized communication readiness and reporting. Ensure team members maintain continuous surveillance of the overall network(s) operation. Prepares briefings and specialized reports as required. Establishes maintenance relationships, agreements and SOPs as required to ensure readiness gaps do not develop. Works with PMs, PEO's and associated support teams to establish training standards on each system and seeks the necessary skill building training, support needs and for current lessons learned on tactics, techniques, and procedures (TTPs), system usage and maintenance improvement.

Ensures the implementation and compliance with various mandates and directives such as the Federal Information Technology Acquisition Reform Act; the 25-Point Implementation Plan to Reform Federal Information Technology Management; the Clinger-Cohen Act; the Federal Information Technology Shared Services Strategy; and all other related guidelines, protocols, bylaws, directives, and regulations. Ensures state maintains full compliance with all aspects of Federal IT laws, executive orders, memoranda, regulations, policies, guidelines, and standards.

2.Directs, coordinates, and oversees work through subordinate supervisors. Advises staff regarding policies, procedures, and directives of higher-level management or headquarters. Selects candidates for subordinate non-supervisory and supervisory positions taking into consideration skills and qualifications, mission requirements, and EEO objectives. Ensures reasonable equity among units of performance standards developed, modified, and/or interpreted and rating techniques developed by subordinate supervisors. Explains performance expectations to subordinate supervisors and employees directly supervised and provides regular feedback on strengths and weaknesses. Appraises performance of

subordinate supervisors and other employees directly supervised and serves as reviewing official on evaluation of non-supervisory employees rated by subordinate supervisors. Approves expenses comparable to within-grade increases, extensive overtime, and employee travel. Recommends awards for non-supervisory personnel and changes in position classification to higher-level managers. Hears and resolves group grievances and employee complaints referred by subordinate supervisors and employees. Initiates action to correct performance or conduct problems of employees directly supervised and reviews and/or approves serious disciplinary actions (e.g. suspensions, removals) involving non-supervisory subordinates. Ensures documentation prepared to support actions is proper and complete. Reviews developmental needs of subordinate supervisors and non-supervisory employees and makes decisions on non-routine, costly or controversial training needs and/or requests. Encourages self-development. Approves leave for subordinate supervisors and ensures adequate coverage in organization through peak workloads and traditional holiday vacation time. Demonstrates sensitivity to ideas of subordinates. Ensures actions taken directly as well as those by subordinate supervisors promote an environment in which employees are empowered to participate in and contribute to effective mission accomplishment. Discharges security responsibilities by ensuring education and compliance with security directives for employees with access to classified or sensitive material. Recognizes and takes appropriate action to correct situations posing a threat to the health or safety of subordinates. Applies EEO/affirmative employment principles and requirements to all personnel management actions and decisions, and ensures all personnel are treated in a manner free of discrimination.

3. Plans, organizes, and oversees the activities of the state G-6. Serves as the State's alternate principal staff office for all facets to include: cybersecurity, automation, telecommunications, information assurance, information plans, policy, integration, budget and records management. Assists in organizational sub-element goals and determines resources needed to maintain the organizational missions and functions. Reviews status of information management related programs, makes planning adjustments and recommends changes. Through branch chiefs and subordinates, determines overall manning needs; secures position authorizations and adjusts for unusual staffing requirements. Reviews guidance/tasking's and devises plans and methods to fund and accomplish the mission.

Provides guidance in defining overall Information Technology (IT) architecture and requirements for the State. Manages the information systems architecture in relation to assigned projects. Reviews, analyzes and verifies feasibility of implementing a total system design, which includes hardware, software, communication systems and networks. Develops and applies technical policy to include standards, protocols, and data administration techniques to effectively integrate and implement information systems. Analyzes information systems to ensure compliance to current commercial and government standards. Determines new and innovative approaches to solve IT problems.

Formulates and defends the IT budget for the Command. Ensures maximum efficiency and cost effectiveness in the utilization of the State's IT, hardware, software, funds and personnel. Defines overall direction and objectives for applicable Management Decision Package (MDEPs). May serve as the Program Manager (PM) when required at the State level Program Budget Advisory Committee. Oversees budget execution through Federal procurement and the Master Cooperative Agreement. Plans, guides, and directs establishment and interpretation of requirements and criteria, ensuring the ability of the systems to meet optimal mission objectives and needs. Interprets and evaluates the effect of higher-echelon directives and their execution. Establishes and/or modifies overall execution procedures and priorities for compliance with higher authority direction while ensuring continued effective and successful implementation programs. Analyzing and continuously monitoring the budget and waiver processes through GFEBS, ITAS, APMS, RMOnline, and cPROBE. Establishes long-range plans and projects and determines priorities and resources. Within the bounds of the Command's overall policy, establishes and/or alters overall execution of policies, procedures and priorities to ensure compliance with higher authority direction is achieved within the constraints of available resources.

4. Monitors, reviews and analyzes program implementations. Manages all aspects of the state Cybersecurity Program to ensure the confidentiality, integrity, availability and non-repudiation of sensitive and classified information and information system resources. Publishes information assurance policy ensuring information assurance policy compliance. Reviews information technology system certification artifacts and provide accreditation recommendations to the installation management and provide information assurance, awareness, training and education. Leads the development and promulgation of

information assurance policies and procedures to ensure that the information assurance program implementation that is consistent with DoD policies, directives and procedures. Assesses the impact of policies, procedures and special projects required to ensure that the agency information assurance program is integrated into the overall State policy, plans operations and strategy in an effective and responsive manner. Responsible for compliance with all applicable Federal, Department of Defense (DoD) and Army regulations (AR) pertaining to information assurance to include, but not limited to the Federal Information Systems Management Act (FISMA), Federal IT Acquisition Reform Act (FITARA), Department of Defense Directive (DoDD) 8500.1, Information Assurance; Department of Defense Instruction (DoDI) 8500.2, Information Assurance Implementation, AR 25-1: Army Knowledge Management and Information Technology Management and AR 25-2: Information Assurance. Ensures all required cybersecurity positions are filled with qualified staff and are on appointment orders.

Manages the Compliance/Governance/Resource Management Branch. As an effort to manage and implement guidance to maintain a successful rating at any time for the Cyber Command Readiness Inspection criteria this branch continuously reviews goals and priorities, ensuring it is financial feasibility and meets the Budget Execution Guidelines. Ensures Configuration Control Boards (CCB) are conducted for change approvals. Maintains access to key IT management systems (APMS, ITAS, eMASS, ATCTC).

Supervises the development and promulgation of information technology policies and procedures to ensure implementation is consistent with DoD policies, directives and procedures. Leads the staffing of information technology policy and assists with developing implementing guidance. Assesses the impact of policies, procedures and special projects required to ensure information management is integrated into the state policy, plans operations and strategy.

5. Represents the command in dealing with state, local, tribal communities and federal government agencies. Promotes coordination, cooperation, and mutual understanding within and between DoD, Army, Air Force, other federal agencies, military departments, defense agencies as well as state, local and tribal communities on various installation management IT programs and initiatives.

Exercises delegated managerial authority to set a series of annual, multi-year or similar types of long-range work plans for in-service and contracted work. Assures implementation of the goals and objectives for the program and functions performed; determines goals and objectives that need additional emphasis, determines, the best approach for resolving budget shortages and plans for long-range staffing needs, including such matters as whether to contract out work. Incumbent assists high level program officials and staff personnel in the development of overall goals and objectives for the assigned staff functions, programs, and program segments by providing expertise and insights and comparable activities that support the development of goals and objectives related to high levels of program management development and formulation.

6. Performs other duties as assigned.

CONDITIONS OF EMPLOYMENT:

1. Must be able to obtain required certifications, as applicable. IAW DoDI 8140, DOD 8570.01M or applicable governing document(s) for Cyber workforce as an IA Technician Level. All certifications are required within 6 months of employment.
2. Must be certified IAW DoD 8570.01-M, Federal Information Security Management Act of 2002, Clinger Cohen Act of 1996 and obtain Special Experience Identifier (SEI) 264, IAW current AF directives. Information Assurance – Technical Level II (IAT II), IAW current AF directives. Position is designated as OV-PL-002 (Cyber Policy and Strategy Planner) within the Defense Cybersecurity Workforce as guided by NIST SP 800-181; National Initiative for Cybersecurity Education, Cybersecurity Workforce Framework. Which establishes the Tasks, Skills, Knowledge and Abilities expected of this position.
3. Must obtain and maintain a TOP SECRET clearance level.