General Position Information

Job Title: Deputy Director, Cybersecurity Group

Position Number: 23204

Position Grade: GS-15

Salary Range: $122,530 - $172,500 (not applicable for detailees)

Vacancy Open Period: 11/10/2021 - 11/25/2021

Position Type: Cadre, Detailee

Who May Apply: Internal ODNI Candidates, Detailees

Division: ODNI/ICCIO

Duty Location: Bethesda, MD

Security Clearance: TS/SCI with CI Polygraph

Travel Required: 0-25% Travel

Relocation Expenses: For new ODNI employees, reimbursement for relocation is discretionary based on availability of funds.

Job Interview Travel: Candidates from outside the Washington, D.C., area may be selected for a telephone, teleconference, or in-person interview. If selected for an in-person interview, any travel or lodging will be at the applicant's personal expense.

Position Information

This is an opportunity for:

- An internal candidate to fill a GS-15 cadre position.
- A Federal Government employee to serve on a two-year reimbursable detail assignment in the ODNI. The detail assignment may be extended an additional year if all parties agree.

Who May Apply

Current GS employees at the same grade or one grade lower as the advertised position grade may apply.

Former members of the Peace Corps may be considered for ODNI employment only if five full years have elapsed since separation from the Peace Corps.

- For a cadre assignment:
    - Current ODNI permanent cadre.
- For a detailee assignment:
    - Current Federal Government employees. (Current GS employees at the same grade or one grade lower as the advertised position grade may apply.)

Salary Determination

- The ODNI uses a rank-in-person system in which rank is attached to the individual. A selected ODNI candidate or other Federal Government candidate will be assigned to the position at the employee's current GS grade and salary.
- A current Federal Government employee, selected for a detail, will be assigned to the position at his or her current grade and salary.

Component Mission

The Intelligence Community (IC) Chief Information Office is responsible for advancing the Intelligence Community's mission by driving secure collaboration, integration, and information sharing; identifying and addressing information enterprise risks; and providing strategic leadership and oversight of the Intelligence Community's enterprise architecture and enterprise information technology.

The Group Deputy Director provides executive management and leadership for the establishment, implementation and maintenance of a comprehensive and effective cyber/information security program to protect the Intelligence Communities classified and unclassified information and information technology assets.

Major Duties and Responsibilities (MDRs)

Provides senior IC leadership with guidance, and expert advice in developing, promoting, and maintaining cyber security controls and performance measures to adequately and cost effectively protect all community cyber critical infrastructure including classified and unclassified information systems and national security systems.

Establishes community cyber/information security policy, standards, and guidelines in accordance with federal law and regulations, Presidential directives, national standards and industry best practices.

Collaborates through the Intelligence Community (IC) Information Security Risk Management Committee (ISRMC), the IC Security Coordination Center and other interagency security officials to establish, maintain and update documentation on the community policy, and IC Chief Information Council recommendations.

Serves as the IC CIO's cyber security liaison to the private sector and federal community.

Facilitates the effective performance of the employees of the group including all of its government and contractor support.

Develops and applies information assurance architecture frameworks, NIST Special Publication 800-53 requirements, translating the requirements into Enterprise security services for large computing environments/enclaves.

Collaborate directly with senior security managers charged with developing security guidelines for the IC.

Provide expert direction and guidance to ensure that information systems that are developed, deployed, operated, implemented, and supported in a manner consistent with INFOSEC policies and procedures.

Mandatory and Educational Requirements

Managing or leading an information/cyber security program for a government or commercial organization.

Superior ability to communicate, both verbally and in writing, complex information in a clear, concise manner that is targeted to and meets the needs of diverse audiences with different perspectives and objectives.

Superior ability to work effectively both independently and in a team or collaborative environment, mentor junior colleagues, and utilize strong organizational and interpersonal problem solving skills.

Risk management experience as a Designated Accreditation Authority (DAA), Risk Executive, Authorizing Official, or Delegated Authorizing Official with responsibility for making organizational Information Technology (IT) risk decisions.

Demonstrated ability to balance security compliance with program cost, schedule, performance, or mission needs.

Lead project teams to ensure project is completed on time, effectively apply team building and coaching techniques, and exchange project or technical information with team members and contractors at formal and informal meetings.

Oversee the work of team members; monitor work activities to ensure counterintelligence and security policies and procedures are followed; provide help or assistance to team members or others when needed; communicate needs and requirements to project team members.

Expert ability to establish regular contact with high-level internal and external resources and have periodic contacts with other offices, supplying or seeking information on specialized and non-specialized matters; excellent use of tact when expressing ideas or opinions to senior leaders, customers, contractors, and other stakeholders.

Key Requirements and How To Apply

Internal ODNI Candidates:

A complete application package must include:

A. **RESUME:** Applicants are encouraged to carefully review the vacancy announcement, particularly the MDRs, and construct their resume to highlight their most significant experience and qualifications relevant to this job opportunity.

B. **PERFORMANCE EVALUATIONS:** Applicants are required to provide their two most recent performance evaluations. A justification is required in the cover letter if the applicant is unable to provide the two most recent evaluations.

C. **VACANCY NUMBER:** Reference the vacancy number in the subject line of the email and on each document submitted.

D. **COVER LETTER:** Applicants must submit a cover letter as a supplement to the resume to elaborate on their qualifications and previous work performed.

Internal ODNI Cadre Candidates must submit an application through the classified JobsDNI website.

For current employees who do not currently have access to internal systems, applications should be sent to either DNI-HR-HRM-TEAMB-Mailbox@cia.ic.gov (classified email system) or Recruitment_TeamB@dni.gov (unclassified email system).

Applications submitted through the classified email system should NOT contain classified information above the TS//SI/TK//NOFORN level.

All attachments should be in Microsoft Word or Adobe PDF format.

Current Federal Employees Applying for a Detail Assignment:

Applicants from federal agencies within the Intelligence Community (IC) may be considered for this position as a reimbursable detailee, if endorsed by the employing agency. Applicants must have current TS/SCI clearances with polygraph or have the ability to obtain one. The ODNI does not conduct polygraphs or provide security clearances for detailees. ***Applicants from within the IC must submit an application through the classified IC Joint Duty Program website.***

Applicants from federal agencies outside the IC must provide:

a. **WRITTEN ENDORSEMENT** from the employing agency concurring with the detail.

b. **RESUME:** Applicants are encouraged to carefully review the vacancy announcement, particularly the MDRs, and construct their resume to highlight their most significant experience and qualifications relevant to this job opportunity.

c. **VACANCY NUMBER:** Reference the vacancy number in the subject line of the email and on each document submitted.

d. **CURRENT SF-50:** Federal Government employees must provide an SF-50, "Notification of Personnel Action" to verify current federal status, position, title, grade, and organization of record. Please disregard if you are not a Federal Government employee.

e. **COVER LETTER:** Applicants must submit a cover letter as a supplement to the resume to elaborate on their qualifications and previous work performed.

WHERE TO SUBMIT: Applications should be sent to either DNI-HR-HRM-TEAMB-Mailbox@cia.ic.gov (classified email system) or Recruitment_TeamB@dni.gov (unclassified email system).

All attachments should be in Microsoft Word or Adobe PDF format.

Applications submitted through the classified email system should NOT contain classified information above the TS//SI/TK//NOFORN level.

All Applicants:

APPLICATION PACKAGES MUST CONTAIN ALL ITEMS LISTED ABOVE. AN INCOMPLETE APPLICATION PACKAGE WILL BE INELIGIBLE FOR CONSIDERATION.

Your application MUST be received by midnight on the closing date of this announcement. Applications received after the closing date will NOT be eligible for consideration.

What To Expect Next

The most highly qualified candidates will be referred to the hiring manager for further consideration and possible interview. We expect to make a selection within 30 days of the closing date of this announcement. Due to the large number of applications received, applicants will be contacted ONLY if they have been selected for an interview.

Agency Contact Information

ODNI Recruitment; Phone: 301-243-1318; Email: Recruitment_TeamB@dni.gov.

Other Information

The ODNI is an equal opportunity employer and abides by applicable employment laws and regulations.

The Office of the Director of National Intelligence (ODNI) requires its employees to be fully vaccinated against COVID-19 pursuant to Executive Order 14043 of the President of the United States. As required, Federal employees must be fully vaccinated against COVID-19 regardless of the employee's duty location or work arrangement (e.g., telework, etc), with exceptions only as required by law. If selected, you will be required to be vaccinated against COVID-19 and submit documentation of proof of vaccination by November 22, 2021 or before appointment or onboarding with ODNI, if after November 22, 2021. ODNI will provide additional information regarding what information or documentation will be needed and how you can request a legally required exception from this requirement. All employees requesting either a medical or religious exception, must follow the Guidelines from the Office of Personnel Management and/or Safer Federal Workforce Task Force.

REASONABLE ACCOMMODATIONS FOR PERSONS WITH DISABILITIES: The ODNI provides reasonable accommodations to otherwise qualified applicants with disabilities. IF YOU NEED A REASONABLE ACCOMMODATION for any part of the application and hiring process, please notify the Intelligence Community Equal Employment Opportunity and Diversity Office Representative by classified email at DNI_Reasonable_Accommodation_WMA@cia.ic.gov and DNI_Diversity_WMA@cia.ic.gov, by unclassified email at DNI_DRA@dni.gov, by telephone at 703-275-3900 or by FAX at 703-275-1217. Your request for reasonable accommodation will be addressed on a case-by-case basis. **PLEASE DO NOT SUBMIT YOUR APPLICATION TO THE EEOD EMAIL ADDRESS. THIS EMAIL IS FOR REASONABLE ACCOMMODATION REQUESTS ONLY. PLEASE SUBMIT YOUR APPLICATION VIA THE EMAIL ADDRESS PROVIDED IN THE 'HOW TO APPLY' SECTION ABOVE.**