



# OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

## General Position Information

**Job Title:** Chief, (Cybersecurity) Risk Management Group

**Position Number:** 26431

**Position Grade:** GS-15

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

**Vacancy Open Period:** 06/03/2021 - 06/24/2021

**Position Type:** Cadre, Detailee

**Who May Apply:** Internal ODNI Candidates, Detailees

**Division:** DNI/ICCIO/CSG

**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 or detailee 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.)



# OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

## 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.

## Major Duties and Responsibilities (MDRs)

- Help lead risk management within the Cybersecurity overseeing Intelligence Community (IC) - wide efforts to safeguard the IC Information Environment (IE) in support of the DNI's Title 44 statutory responsibilities and leads development and implementation of a comprehensive IC IE safeguarding strategy.
- Enables the IC Mission through the effective delivery of cybersecurity risk assessment, authorization, compliance/performance analysis, and mitigation services.
- Serves as a Cybersecurity Advisor to the IC CISO on all Information System Security matters and is a Subject Matter Expert in applying ICD 503, CNSS 1253, NIST SP 800-53, the Risk Management Framework (RMF) and the application of adequate security controls across the entirety of the IC IE.
- Skillfully executes functions that include; information security policy interpretation, review of system security Bodies of Evidence (BOE) comprising the System Security Plan (SSP), Security Assessment Reports (SARs), Risk Assessment Reports (RARs), Security Concept of Operations (SECONOP), Plan of Action and Milestone (POA&M); provides critical thinking in determining if security controls are sufficient to protect all levels of classified information in system design and risk determination, negotiates among various technical and management parties (at all levels), and formulates positions across a wide range of cybersecurity issues.
- Provides senior level analysis and review of risk considerations (mission, security, and costs tradeoffs) in context of IC and agency missions, able to review Performs and provides risk tradeoff analysis to implement the policies, processes, models, assessments, and standards needed to recommend risk acceptance authorization for complex systems and mission enablement.



# OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

- Define and develop information security requirements and engineering solutions for new systems and plan, define, and review system security plans.
- Provides the information system owners detailed and constructive recommendations for correction, along with references to appropriate government regulations and explanations and desired specific outcome(s) of the corrections.
- Collaborate directly with senior security managers charged with developing security guidelines for the IC.
- Lead and manage complex computer engineering projects or programs that may have ill-defined requirements, ambiguity, parallel tasks, multiple dependencies, high risks, and multiple interfaces; manage the design, construction, testing, and implementation of technical and functional specifications; provide technical oversight and initiate, plan, implement, and coordinate activities throughout the life of the project.

## **Mandatory and Educational Requirements**

- Superior ability to balance responsibilities among project activities; ability to manage transitions effectively from task to task, adapting to varying customer needs.
- Superior ability to develop or implement information systems security plans and procedures.
- 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 establish regular contact with high-level internal and external resources and customers, supplying or seeking information on security programs and issues; superior use of tact when expressing ideas or opinions to senior leaders, customers, contractors, and other stakeholders.
- Ability to examine available data (which may be incomplete), applying the relevant facts aided by past experience and in-depth knowledge, and make decisions and/or arrive at conclusions that are fundamentally sound.
- Demonstrated ability to balance security compliance with program cost, schedule, performance, and/or mission needs.



# OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

- Knowledge of network and information security architectures and systems security engineering concepts, including topology, protocols, services, components, and principles (e.g., application of defense-in-depth).
- Experience with virtual and cloud computing technologies and concepts and experience with developing system security requirements, documentation, and network and workflow diagrams.

## Desired Requirements

- Experience: One year of specialized experience at the next lower GS-grade (or equivalent). IT-related experience may be demonstrated by paid or unpaid experience and/or completion of specific, intensive training (for example, IT Certification). IT-related experience demonstrating each of the four competencies (Attention to Detail, Customer Service, Oral Communication, and Problem Solving).
- Education: Degree in computer science, engineering, information science, information systems management, mathematics, operations research, statistics, or technology management or degree that provided a minimum 24 semester hours in one or more of the fields identified above and required the development or adaptation of applications, systems or networks.
- Certifications/Licenses: Certified Information System Security Professional or other equivalent information security certification recommended, but not required.

## Key Requirements and How To Apply

Internal ODNI Candidates:

A complete application package must include:

- 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.
- 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.
- VACANCY NUMBER:** Reference the vacancy number in the subject line of the email and on each document submitted.
- 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:** *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](mailto:DNI-HR-HRM-TEAMB-Mailbox@cia.ic.gov) (classified email system) or [Recruitment\\_TeamB@dni.gov](mailto:Recruitment_TeamB@dni.gov) (unclassified email system).



# OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

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

## **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. **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.
- d. **VACANCY NUMBER:** Reference the vacancy number in the subject line of the email and on each document submitted.
- e. **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.
- f. **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](mailto:DNI-HR-HRM-TEAMB-Mailbox@cia.ic.gov) (classified email system) or [Recruitment\\_TeamB@dni.gov](mailto: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.



# OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

L E A D I N G I N T E L L I G E N C E I N T E G R A T I O N

## Agency Contact Information

ODNI Recruitment; Phone: 301-243-1318; Email: [Recruitment\\_TeamB@dni.gov](mailto:Recruitment_TeamB@dni.gov).

## Other Information

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

**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](mailto:DNI_Reasonable_Accommodation_WMA@cia.ic.gov) and [DNI\\_Diversity\\_WMA@cia.ic.gov](mailto:DNI_Diversity_WMA@cia.ic.gov), by unclassified email at [DNI\\_DRA@dni.gov](mailto: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.**