



# 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:** 30095 - Assessment Oversight Lead, DNI/ICCIO- GS-15

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

**Vacancy Open Period:** 01/07/2021 - 01/28/2021

**Position Type:** Cadre, Detailee

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

**Division:** DNI/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 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 than 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.
  - Current ODNI Staff Reserve Employees. (A staff reserve employee who currently occupies this position may not 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

- Current Federal Government employees. (Current GS employees at the same grade or one grade lower than the advertised position grade may apply.)
- Candidates outside the Federal Government.
- For a detailee assignment:
  - Current Federal Government employees. (Current GS employees at the same grade or one grade lower than 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.
- For a selected non-Federal Government candidate, salary will be established within the salary range listed above, based on education and experience.
- 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)

- Lead, guide and oversee professional staff performing work in various cybersecurity specialties, and in resolving major conflicts in policy and program objectives.
- Lead, guide, and oversee staff in the analysis of the strengths and weaknesses of complex cybersecurity programs, processes, and procedures and develop new strategies for resolving complex problems or improving overall performance.
- Lead and oversee staff in developing strategic and tactical plans to support Intelligence Community (IC) cybersecurity initiatives; guide and lead the development, implementation, and evaluation of security programs in response to IC directives and/or mission requirements.
- Plan for new or far-reaching cybersecurity program requirements, and lead interagency study groups for resolving problems in existing cybersecurity systems and programs requiring innovative solutions.
- Advise top level agency cybersecurity and subject-matter experts on new developments and advances in cybersecurity techniques.
- Make authoritative recommendations on methods for enhancing efficiency of cybersecurity systems through modifications and applications of evolving technology.



- Evaluate and make authoritative recommendations concerning overall plans and proposals for major agency and interagency security projects.
- Implement IC wide guidance in agency standards, guidelines, or policies for major IC cybersecurity programs.
- Analyze, plan, schedule, and coordinate the development of legislation and cybersecurity policy issuances that direct the course of cybersecurity programs in the IC community and others involved in sensitive and secure work performed in or for the Federal Government.
- Serve as an expert authority resolving problems or issues concerning several phases of cybersecurity policy, development and implementation for a variety of programs in one or more fields of cybersecurity.
- Lead, cultivate, and maintain productive working relationships with security colleagues, IC senior leadership to share information of interest, explain the specifics of security programs and procedures, and, when appropriate, present, justify, defend, negotiate, and/or settle matters involving significant or controversial issues.
- Assess performance, collaborate and oversee goal setting, and provide feedback on personal development for assigned team members.
- Serve as a member on interagency committees or in national security organizations involved in reviewing, analyzing, developing and issuing national policy directives and drafting legislation affecting security policies and programs throughout the Government and private sectors.

## **Mandatory and Educational Requirements**

- Expert knowledge of general cybersecurity administration programs and mastery of cybersecurity specialty.
- Expert knowledge of IC security regulations, policies, and procedures in order to address and resolve IC security issues, violations, and questions.
- Expert ability to develop and effectively manage a complex cybersecurity program, assess customer requirements, identify dependencies, and manage and mitigate risks.
- Expert program management, analytic, and critical thinking skills, including a superior ability to oversee cybersecurity program assessments, identify needs and requirements, and develop process improvement recommendations for the successful implementation of IC security programs.
- 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.
- Superior ability to establish regular contact with high-level internal and external resources and customers, supplying or seeking information on cybersecurity programs and issues; superior use of tact when expressing ideas or opinions to senior leaders, customers, contractors, and other stakeholders.
- Superior ability to listen to, clarify, and convey an understanding of others' ideas, comments, and questions, and integrate and build upon diverse opinions in a manner that encourages the formation of integrated solutions and positions.



- Expert ability to direct taskings, assess and manage performance, collaborate on goal setting, and support personal and professional development of all levels of personnel.

## 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: Cybersecurity certifications (CISSP, CISM, CEH, etc.) or the ability to obtain.

## 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\\_coo\\_hrm\\_hr\\_ops\\_team\\_b\\_wma@cia.ic.gov](mailto:dni_coo_hrm_hr_ops_team_b_wma@cia.ic.gov) (classified email system) or [Recruitment\\_TeamB@dni.gov](mailto:Recruitment_TeamB@dni.gov) (unclassified email system). Applicants experiencing technical issues should contact the HR POC for guidance. Applicants submitting via JWICS are requested to submit their materials to [zackern@dni.ic.gov](mailto:zackern@dni.ic.gov) (Natalia Z.), and [mcbrije@dni.ic.gov](mailto:mcbrije@dni.ic.gov) (Jerry M.) in lieu of the group address above.

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



# 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

## 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\\_COO\\_HRM\\_HR\\_OPS\\_TEAM\\_B\\_WMA@cia.ic.gov](mailto:DNI_COO_HRM_HR_OPS_TEAM_B_WMA@cia.ic.gov) (classified email system) or [Recruitment\\_TeamB@dni.gov](mailto:Recruitment_TeamB@dni.gov) (unclassified email system). Applicants submitting via JWICS are requested to submit their materials to [zackern@dni.ic.gov](mailto:zackern@dni.ic.gov) (Natalia Z.) and [mcbrije@dni.ic.gov](mailto:mcbrije@dni.ic.gov) (Jerry M.) in lieu of the group address above.

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.



# 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

## 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](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 703-275-3799 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 EEOC 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.**