General Position Information

Job Title: 30271 - Team Lead, Cybersecurity Analysis and Reporting Team - GS-14

Salary Range: $117,191 - $152,352 (not applicable for detailees)

Vacancy Open Period: 12/19/2019 – 12/18/2020

Position Type: Cadre, Detailee

Who May Apply: Internal ODNI Candidates, Detailees

Division: CIO/CSD

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

***** OPEN UNTIL FILLED: This announcement will be open until the position is filled. Cut off points are scheduled in two-week increments. After each cut-off point, all compliant applications received during the previous two weeks will be reviewed for consideration.*****

This is an opportunity for:

- An internal candidate to fill a GS-14 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 as 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 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 Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC). The DNI also acts as the principal advisor to the President and the National Security Council for intelligence matters related to national security; and oversees and directs the implementation of the National Intelligence Program. The DNI leads intelligence integration and forges an intelligence community that delivers the most insightful intelligence possible.

The Deputy Director of National Intelligence for Enterprise Capacity (DDNI/EC) is responsible to the DNI for all matters pertaining to IC resources, workforce, systems, technology and infrastructure, with five reporting components: Acquisition, Procurement and Facilities, IC Chief Financial Officer, IC Chief Human Capital Officer, IC Chief Information Officer, and Systems & Resource Analyses.

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)

- CSD oversees IC-wide efforts to safeguard the IC IE in support of the DNI's Title 44 statutory responsibilities. With a focus on security aspects of the IC IE, CSD utilizes proactive oversight and management levels of governance, policy, standards, architecture, engineering, risk management, testing investment, and reporting to drive a secure, robust, and integrated IC IE aligned with IC mission-related objectives and strategies. The Director of CSD is dual-hatted as the IC Chief Information Security Officer (IC CISO).
- Serve as Lead, Cybersecurity Assessment and Reporting Team within the Risk Management Group, Cybersecurity Division (CSD), leading the execution, documentation, and authorization processes necessary to assure that new and current information technology systems meet the IC's Information Assurance requirements.
- Enables the Intelligence Community (IC) Mission through the effective execution of the Risk Management Framework (RMF) and the application of adequate security controls across the entirety of the IC Information Environment (IE).

- Ensures that the appropriate management and operational security posture is maintained for information systems.
- Serves as a principal advisor on all info system security matters and is a subject matter expert in applying ICD 503, CNSS 1253, and NIST SP 800-53.
- Executes functions that include; info security policy interpretation, reviewing security control assessments, providing briefings and presentations to senior audiences, negotiating among different parties, formulating 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 missions, interpreting Security Assessment Reports (SARs), Risk assessment Reports (RARs), providing critical thinking in applying security controls to system design and risk determinations.
- 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.
- Define and develop information security requirements and engineering solutions for new systems and plan, define, and review system security plans.
- Directly support more senior security managers charged with developing security guidelines for the IC and ensuring that security processes are compliant with appropriate federal requirements.
- 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.
- Conducts activities and works with government personnel, supervisors, contractors, and liaise with other government agencies throughout the DoD and the IC.

Mandatory and Educational Requirements

- Ability to examine available data, applying the facts and own experience, and making decisions that generally prove sound.
- Demonstrated ability to balance security compliance with program cost, schedule, performance, or mission needs.
- Developing and/or applying Information Assurance/ Cybersecurity principles, policies, practices, standards, and controls, to include application of the Risk Management Framework (RMF), relevant to confidentiality, integrity, availability, authentication, and non-repudiation.
- Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
- Knowledge of network security architecture and systems security engineering concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth).

- Experience with virtual and cloud computing technologies and concepts, to include DevSecOps; experience with developing system security requirements.

- Demonstrated ability to establish regular contact with high-level internal and external resources and customers, supplying or seeking information on security programs and issues; demonstrated ability to tactfully express ideas or opinions to senior leaders, customers, contractors, and other stakeholders.

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.

- Certification/Licenses: Certified Information System Security Manager (CISSM) and/or Certified Information System Security Professional (CISSP) preferred.

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.

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_TM_HR_OPS_TEAM_B_WMA@cia.ic.gov (classified email system) or Recruitment_TeamB@dni.gov (unclassified email system). Applicants experiencing technical issues may submit their

application via email to either email system. Applicants submitting via JWICS are requested to submit their materials to both majettm@dni.ic.gov (Maya M.) and mcginlj@dni.ic.gov (Johnny 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.

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_TM_HR_OPS_TEAM_B_WMA@cia.ic.gov (classified email system) or Recruitment_TeamB@dni.gov (unclassified email system). Applicants submitting via JWICS are requested to submit their materials to both majettm@dni.ic.gov (Maya M.) and mcginlj@cia.ic.gov (Johnny 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.

To verify receipt of your application package ONLY, you may call 301-243-1318.

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.

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_COO_TM_EEOD_RA_WMA@cia.ic.gov, by unclassified email at DNI-EEOD_WMA@cia.ic.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.**