General Position Information

Job Title: PF280 - IT Engineer (Deputy Lead, Intelligence Community (Cybersecurity) Technical Assessment Team - GS-14

Salary Range: $99,172 - $152,352 (not applicable for detailees)

Vacancy Open Period: 05/01/2019 – 05/29/2019

Position Type: Cadre, Detailee

Who May Apply: Internal ODNI Candidates, Detailees

Division: CIO/CIO

Duty Location: Reston, VA

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-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 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.
- 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.
- 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 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, the National Security Council, and the Homeland Security Council for Intelligence matters related to the 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 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)

- Serve as Associate Lead for the Intelligence Community (Cybersecurity) Compliance Assessment Team within Information Assurance Division (IAD) leading the strategic planning and management of technical security compliance assessment and "Blue Team" programs and activities. The associate will lead risk management efforts.
- Identifies systemic security issues based on the analysis of vulnerability and configuration data.
- Apply penetration testing principles, tools, and techniques (e.g., metasploit, neosploit).
- Maintains knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- Provides technical advice on network security architecture and systems security engineering concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth).

- Continuously looking for ways to improve results, showing resourcefulness, and pushing for excellence.
- Participate in the design, evaluation, selection, implementation, and support of development and production support tools and platforms.
- Lead the development of interoperability test plans, building upon the component test plans developed by the service providers; coordinate the testing of new capabilities with other elements to ensure that all equities are covered in the test process; serve as the Independent Validation and Verification test director, conducting the technical functionality testing and coordinating the activities of other elements as they conduct the Analysis and Accreditation testing and the user functionality test.

Mandatory and Educational Requirements

- Demonstrated ability to adapt to new demands or information and handling situations with multiple variables and unknowns successfully.
- Extensive knowledge in managing an Information Assurance/ Cybersecurity program, project, or process employing related skills such as objective and requirements development, task break out, developing schedules and budgets, identifying risks and opportunities, and identifying required resource.
- Experience with virtual and cloud computing technologies and concepts; experience with developing system security requirements.
- Experience 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.
- Demonstrated creative thinking, problem solving, and analytical techniques.
- Extensive experience in cross community complex programs and making recommendations to improve products and services; considerable ability to deal with service failures and prioritize customer needs.
- Demonstrated 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.
- Demonstrated ability to quickly identify and apply new technologies, methodologies, and technical languages.

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:

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: 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 *joswida@dni.ic.gov (Daniel J.), mitchsl*@cia.ic.gov *(Stephanie M.), and* perryad@dni.ic.gov *(Adriane P.)* 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: 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 *joswida@dni.ic.gov (Daniel J.),* mitchsl@cia.ic.gov *(Stephanie M.), and* perryad@dni.ic.gov *(Adriane P.)* 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 301-243-0704 or by FAX at 301-243-1200. 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.**