General Position Information

Job Title: PF245- Chief, DNI/ICCIO/MRG- GS-15

Salary Range: $142,701 - $170,800 (not applicable for detailees)

Vacancy Open Period: 10/20/2020 - 11/04/2020

Position Type: Cadre, Detailee

Who May Apply: Internal ODNI Candidates, Detailees

Division: DNI/ICCIO/MRG

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.

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.)
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

CSG 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, CSG utilizes proactive oversight and management levers of governance, policy, standards, architecture, engineering, risk management, and reporting to drive a secure, robust, and integrated IC IE aligned with IC mission-related objectives and strategies. The Director of CSG is dual-hatted as the IC Chief Information Security Officer (IC CISO).

### Major Duties and Responsibilities (MDRs)

- Serve as Chief within the Office of the Intelligence Community Chief Information Officer (IC CIO) Cybersecurity Division.
- Lead all on security and technical related matters, formulating integrated policies for information assurance principles to guide secure technology decisions.
- Enable Intelligence Community (IC) mission through the development of system security concepts and capabilities that improve the safeguarding IC data and systems.
- 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.
- Lead in the drafting and coordination of all IC CIO technical specifications, and policies, in accordance with IC's Enterprise Architecture to ensure security practices are streamlined and then integrated into transformed business practices.
• Lead in technical research and the application of best practices and processes for capturing, refining, and assisting in prioritization of security requirements based on risk, system security engineering principles, and mission requirements.

• Lead in the collection of cybersecurity requirements and facilitate the translation of these requirements into secure technical solutions that can be understood by adopters, implementer’s, and developers.

• Provide guidance to customers about applicability of information systems security solutions to meet mission needs.

• Oversee the effective integration and interoperability of disparate cybersecurity related capabilities developed by separate service providers.

• Consult with customers to gather and evaluate security architectures, designs, and system configuration information that facilitate secure missions systems.

• Liaison and represent IC CIO interest and equities at inter-agency forums established to coordinate and develop National-level Cyber Security policies, standards, procedures, guidelines, and advisories for the protection of sensitive government information.

• Typical functions include cybersecurity policy interpretation, providing briefings and presentations to senior audiences, negotiating among different parties, formulating positions across a wide range of information security issues.

**Mandatory and Educational Requirements**

• Expert experience in cross community complex programs and making expert recommendations to improve products and services; considerable ability to deal with service failures and prioritize customer needs.

• Superior ability to manage 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 resources.

• Superior interpersonal, organizational, and problem-solving skills, including a demonstrated ability to work effectively both independently and in a team or collaborative environment and to lead and mentor junior colleagues.

• Expert 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 listen to, clarify, and convey understanding of others’ ideas, comments, and questions as well as to integrate and build upon diverse opinions in a manner that encourages the formation of integrated solutions and positions.

• Expert ability to use knowledge and experience to look at a situation objectively, setting aside any biases, and determining the best long-term solution

• Superior ability to develop and/or applying Information Assurance/ Cybersecurity principles, policies, practices, standards, and controls relevant to confidentiality, integrity, availability, authentication, and non-repudiation.

• Superior ability to perform thorough work and conscientious about attending to detail.
Expert knowledge of network security architecture and systems security engineering concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth).

Expert knowledge of design, development, and inter-connectivity in problem analysis, structured analysis and design, and or programming techniques.

Expert ability to quickly identify and apply new technologies, methodologies, and technical languages.

Expert ability to capture and refine information security requirements and ensure the requirements are integrated into information technology component products and information systems through purposeful security architecture, design, development, and configuration.

Expert ability to monitor trends in development, including the ability to assess the viability of competing technologies and recommend the adoption of emerging technologies.

### 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 Systems Security Professional (CISSP) or equivalent certification; and/or ability to obtain certifications.

### 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 should contact the HR POC for guidance. Applicants submitting via JWICS are requested to submit their materials to zackern@dni.ic.gov (Natalia Z.) and 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.

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 zackern@dni.ic.gov (Natalia Z.) and 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.

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_Reasonable_Accommodation_WMA@cia.ic.gov and DNI_Diversity_WMA@cia.ic.gov, by unclassified email at DNI_DRA@dni.gov, by telephone at 703-275-3799 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 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.