



General Position Information

Job Title: Deputy Information System Security

Position Number: CO113

Position Grade: GS14

Salary Range: \$126,233 - \$164,102 (not applicable for detailees)

Vacancy Open Period: 05/10/2022 – 05/25/2022

Position Type: Cadre

Who May Apply: Internal ODNI Candidates

Division: DNI/COO

Duty Location: McLean, 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.

Who May Apply

Current ODNI permanent employees at the same grade as the advertised position grade may apply.

- For a cadre assignment:
 - Current ODNI permanent cadre.

Salary Determination

- The ODNI uses a rank-in-person system in which rank is attached to the individual. A selected ODNI 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 assignment, will be assigned to the position at his or her current grade and salary.



Component Mission

The Office of the Director of National Intelligence (ODNI) Chief Operating Officer (COO) has the responsibility for advising the Director of National Intelligence (DNI) and administering the DNI's vision and direction to the ODNI enterprise. This includes synchronizing policy, plans, procedures, and cross-functional issues. The COO is responsible for integrating the ODNI staff to execute all missions and tasks designated by the DNI and the Principal Deputy Director of National Intelligence (PDDNI), and for overseeing the internal management of the ODNI.

The COO oversees all ODNI business operations, including such areas as human resources, diversity & inclusion, finance and budget, information technology, security, facilities, and information management. The COO is also responsible for ODNI's emergency planning.

The ODNI Chief Information Office (OCIO) oversees the effective acquisition, management, and safeguarding of the ODNI's information systems and resources, including performing all necessary functions and responsibilities associated with the internal management and oversight of ODNI information systems. OCIO has three groups: Enterprise Technology Integration, Cyber Security, and Enterprise Plans & Resource Management. OCIO also oversees ODNI's contracted service providers including IT Services Group.

Major Duties and Responsibilities (MDRs)

Execute functions that include program management, budget execution, application/tool selection and general contract direction.

Serve as an Information Systems Security Manager (ISSM) within Office of Director of National Intelligence (ODNI), with responsibility for developing strategic plans and managing Information Security (INFOSEC) programs and activities.

Plan, develop, implement, and maintain INFOSEC programs within ODNI; review, approve, and develop security plans for ODNI and develop security measures to safeguard information against unauthorized modification, destruction, or disclosure.

Plan, develop, deploy, and operate information systems in a manner that is consistent with INFOSEC policies and procedures.

Plan, develop, and implement ODNI's security processes to ensure they operate effectively and are compliant with the Federal Information Systems Security Management Act (FISMA) and other relevant policies, guidelines, and procedures.

Plan, develop, and implement ODNI's security policy and technical requirements for system design and operations; serve as an information security consultant for both internal ODNI components and Intelligence Community (IC) stakeholders.

Define and develop information security requirements and engineering solutions for new systems and guide the definition and review of system security plans.

Represent ODNI at IC-wide INFOSEC forums (i.e., the Information Security Program Council (IPC)) and other critical collaborative security specific forums and discuss ODNI's position on key information security issues.



Collaborate directly with senior security managers charged with developing security guidelines for the IC.

Cultivate and maintain productive working relationships with cyber security colleagues, IC counterparts, and ODNI senior leadership to share information of interest, explain the specifics of cyber security programs and procedures, and, when appropriate, present, justify, defend, negotiate, and/or settle matters involving significant or controversial issues.

Mandatory and Educational Requirements

Degree in cyber security, computer science, engineering, information science, information systems management, mathematics, operation research, statistics or technology management or equivalent work experience in one of the listed fields.

Extensive knowledge of information technology infrastructure including operating systems, major application systems, and network architecture, to include virtual and cloud computing technologies.

Extensive knowledge of information technology security environment, business requirements, and risks.

Extensive knowledge of INFOSEC policies, procedures, and practices, as well as the implications of those policies on component Information Technology (IT) systems and security issues.

Program management, analytic, and critical thinking skills, including a superior ability to conduct INFOSEC program assessments, identify needs and requirements, and develop process improvement recommendations for the successful implementation of ODNI's INFOSEC programs.

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 work effectively both independently and in a team or collaborative environment, mentor junior colleagues, and utilize strong organizational and interpersonal problem solving skills.

Demonstrated 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.

Demonstrated 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.

Desired Requirements

Extensive familiarity with ICD 503, CNSSI 1253, NIST SP 800-37 and NIST SP 800-53.

Extensive familiarity with ODNI organization, hierarchy and structure.

Certified Information System Security Professional (CISSP) or other technical IT certification.



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. **POSITION NUMBER:** Reference the position 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-HRM-Vacancies-Mailbox@cia.ic.gov (classified email system) or HRM-HR-OPS-VACANCY-TEAM@dni.gov (unclassified email system). Applicants experiencing technical issues may submit their application via email to either email system.

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 703-275-3888

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: 703-275-3888; Email: HRM-HR-OPS-VACANCY-TEAM@dni.gov.



Other Information

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

COVID-19 Vaccination Requirement: To ensure compliance with an applicable nationwide preliminary injunction, which may be supplemented, modified, or vacated, depending on the course of ongoing litigation, the federal government will take no action to implement or enforce the COVID-19 vaccination requirement pursuant to Executive Order 14043 on Requiring Coronavirus Disease 2019 Vaccination for federal employees. Therefore, to the extent a federal job announcement includes the requirement that applicants must be fully vaccinated against COVID-19 pursuant to Executive Order 14043, that requirement does not currently apply.

Federal agencies may request information regarding the vaccination status of selected applicants for the purposes of implementing other workplace safety protocols, such as protocols related to masking, physical distancing, testing, travel, and quarantine.

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 Reasonable Accommodation Office Representative by classified email at DNI_Reasonable_Accommodation_WMA@cia.ic.gov by unclassified email at DNI_DRA@dni.gov, by telephone at 703-275-3900 or by FAX at 703-275-1277 . Your request for reasonable accommodation will be addressed on a case-by-case basis.

THIS EMAIL IS FOR REASONABLE ACCOMMODATION REQUESTS ONLY. PLEASE SUBMIT YOUR APPLICATION VIA THE EMAIL ADDRESS PROVIDED IN THE 'HOW TO APPLY' SECTION ABOVE.