General Position Information

Job Title: 29575 – Cyber Threat Integration Officer - GS-14

Salary Range: $102,663 - $157,709 (not applicable for detailees)

Vacancy Open Period: 04/21/2020 – 05/12/2020

Position Type: Cadre

Who May Apply: Internal ODNI Candidates

Division: DNI/CTIIC/AIS

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.
- 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 or one grade lower than 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 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, 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 Cyber Threat Intelligence Integration Center (CTIIC) builds understanding of foreign cyber threats to US national interests to inform decision-making by federal cyber centers, departments and agencies, and policymakers. CTIIC works with its partners to integrate threat intelligence and related information from the network defense, intelligence, and law enforcement communities; facilitate information-sharing; lead community analysis of cyber threat; and support interagency planning to develop whole-of-government approaches against cyber adversaries.

Major Duties and Responsibilities (MDRs)

ODNI's Cyber Threat Intelligence Integration Center (CTIIC) is seeking analysts from any discipline who have strong tradecraft and interpersonal skills to join our Analytic Integration Section in leading and integrating IC analysis of foreign cyber threats from both government and non-state actors.

Cyber is increasingly infused in all national security topics, making this position an excellent opportunity for analysts with background in regional or functional relevant national security issues to gain expertise with the cyber threat mission and customer set. Experience with cyber issues is of course welcome but not a requirement. CTIIC is committed to developing a joint duty workforce through training and other opportunities, and seeks personnel who can contribute analytic talent and other related expertise to our mission.

As with all analysis, CTIIC works to tell the most important stories to a wide range of customers, and in doing so, make the cyber story approachable in a way that allows our customers to understand the significance of the information and identify opportunities to take action in the interests of US national security.

CTIIC provides direct support to the NSC Staff and as such provides opportunities to gain insight into the development of cyber policy. CTIIC also works across the IC and other USG agencies with interests in US critical infrastructure, providing opportunities for analysts to develop a diverse range of contacts and gain exposure to a broad range of USG activities and perspectives.
The selected applicant will:

- Plan, research, and develop integrated community analysis of significant cyber threat topics, trends, or incidents to inform policymakers, the Intelligence Community (IC), law enforcement, and the Office of the Director of National Intelligence (ODNI).
- Drive community collaboration and enhance understanding of cyber threats among US stakeholders through Community of Interest (COI) development, information sharing, briefings, and multidisciplinary analysis of adversary use of cyber means to achieve strategic objectives.
- Lead US cyber community thinking on emerging cyber issues that drive IC/federal cyber community analysis and action; lead discussions on near-term cyber topics of interest to policymakers and federal cyber partners in coordination with the NIC.
- Provide integrated all-source analysis of cyber threat intelligence and information from the intelligence, network defense, law enforcement, and response components of the federal cyber community to support whole of government approaches against cyber adversaries.
- Plan, prepare, and present written and oral briefings to senior internal and external customers and analytic counterparts on significant intelligence issues; clearly articulate complex concepts to non-expert customers and tailor the product to correspond to customer needs.
- Share intelligence updates and information with federal cyber partners and provide input to cyber community plans, products, and engagements.
- Improve intelligence integration by writing finished intelligence that provide strategic context to operators and senior decision-makers alike, thus incentivizing cooperation.
- Address analytic gaps and points of disagreement across the IC/federal cyber community.
- Cultivate communities of interest and identify key internal and external sources of information that meet customer and self-derived needs.
- Cultivate and maintain collaborative working relationships with colleagues, experts, IC members, policy committees, and law enforcement agencies, as appropriate, and leverage these relationships to share information of interest.
- Attend relevant internal and external training, seminars, or conferences that will contribute to analytic expertise.
- Works independently with broad lateral guidance by senior management.

**Mandatory and Educational Requirements**

- Demonstrated analytic and critical thinking skills, including superior ability to think strategically.
- Demonstrated ability to effectively plan, research, develop, and author high-quality, complex analyses, studies, projects, assignments, and briefings on key US foreign policy and national security objectives focused on a specific region or transnational issue for IC consumers and senior policymakers.
- Superior ability to apply knowledge of ODNI, IC, military and law enforcement organizations in order to provide tailored responses that meet customer needs.
- Demonstrated knowledge of analytic tradecraft and superior ability to communicate intelligence information and judgments to generalists as well as specialists.
- Demonstrated ability to produce analytic finished intelligence related to the subject matter issue, either as lead analyst or manager of analysts.
- Demonstrated ability to lead and promote the development and use of a broad range of methodological tools and approaches to research, analyze, and present data.
• Demonstrated ability to maintain and develop regular IC contacts for analytic exchange and collaboration.
• Superior ability to support group decisions and solicit perspectives from coworkers.
• Demonstrated ability to promote information sharing practices across the ODNI and IC.
• Demonstrated ability to execute senior-level guidance in a fast-paced environment and accomplish strategic goals using metrics and other measures of effectiveness to track progress.
• Demonstrated interpersonal, organizational, and problem-solving skills, negotiating, and resolving significant and controversial issues.
• Demonstrated ability to work effectively both independently and in a team or collaborative environment, and mentor junior colleagues.
• Creative problem-solving skills and initiative in carrying out mission responsibilities.

Desired Requirements

• Experience: Five years of related work experience.
• Education: Bachelor's degree in subject matter area, or closely related discipline.
• Experience working Iran/Middle East, Russia, North Korea or China are highly desirable.

Key Requirements and How To Apply

Internal ODNI Cadre 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. 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_D_WMA@cia.ic.gov (classified email system) or Recruitment_TeamD@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 micheao@dni.ic.gov (Michelle O.) and zackern@dni.ic.gov (Natalia Z.) in lieu of the group address above.
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.

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.

To verify receipt of your application package ONLY, you may call 703-275-3663.

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: 703-275-3663; Email: Recruitment_TeamD@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.