

**Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications
Vacancy Announcement**

Job Title: IT Specialist (INFOSEC)

Job Announcement Number: **ScdA-CYB003-CS-15**

SALARY RANGE: \$42,399 - \$79,936 / Per Year

(Locality pay may apply as appropriate)

OPEN PERIOD: Thursday, January 22, 2015 – Friday, January 30, 2015

SERIES & GRADE: GS-2210-9/11/12

POSITION INFORMATION: Temporary, Not To Exceed One Year
Excepted Service Appointment

PROMOTION POTENTIAL: 12

DUTY LOCATIONS: Few vacancies in the following locations:
Arlington, VA
Idaho Falls, ID
Pensacola, FL

WHO MAY APPLY: United States Citizens and Status Candidates

SECURITY CLEARANCE: Suitability, Secret, Top Secret or Top Secret/SCI

JOB SUMMARY:

Are you interested in a cyber-temporary appointment where your primary purpose will be to ensure the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, and enhancement of information systems security programs, policies, and procedures? Then consider joining the Office of Cybersecurity and Communications (CS&C), National Protection and Programs Directorate (NPPD), Department of Homeland Security (DHS).

CS&C is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm strategic assets. CS&C works to prevent or minimize disruptions to our critical information infrastructure in order to protect the public, the economy, government services, and the overall security of the United States. It does this by supporting a series of continuous efforts designed to further safeguard federal government systems by reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats.

We are actively recruiting candidates skilled in:

- Cyber Incident Response and Incident Handling
- Cyber Risk and Strategic Analysis
- Vulnerability Detection and Assessment
- Intelligence and Investigation
- Networks and Systems Engineering
- Digital Forensics and Forensics Analysis
- Software Assurance

Who May Be Considered: Applications will be accepted from All US Citizens and Status Candidates.

This announcement is issued under the DHS Schedule A Cybersecurity Authority (Sch. A, 213.3111). Selectee(s) will receive an Excepted Service Appointment.

Additional selections may be made from this announcement should the need arise.

TRAVEL REQUIRED

- Overnight travel of 1-5 nights per month may be required.

RELOCATION AUTHORIZED

- No

KEY REQUIREMENTS

- U. S. Citizenship is required.
- Must be able to obtain and maintain a Secret, Top Secret or Top Secret/SCI security clearance.
- Appointment is subject to the availability of funds.
- May be required to work after-hours emergency response
- May be subject to random drug testing

DUTIES:

- Work under the direction of senior technical and management staff to plan, develop, implement, and evaluate specific aspects of projects involving use of IT systems.
- Integrate security programs across disciplines.
- Define the scope and level of detail for security plans and policies; applicable to the security program.
- Assess new systems design methodologies to improve software quality.
- Research, analyze, write, review, and evaluate security incident response policies.
- Review proposed new systems, networks, and software designs for potential security risks.
- Resolve integration issues related to the implementation of new systems with the existing infrastructure.

QUALIFICATIONS REQUIRED:

To qualify for this position at the GS-9 level, you must have the following:

Basic knowledge of concepts and practices of processing digital information and operating systems; Basic knowledge of industry standard methods and materials used to assist in incident response and mitigation; Basic knowledge of industry standard forensic tools, and foundational experience in conducting forensic analysis and utilizing databases and sources to research known malware and define its characteristics; Basic knowledge of what constitutes a threat to a network; and protocols for reporting network alerts from various sources within the enterprise to management; Foundational experience in requesting digital media and providing it to incident response/field support teams for further analysis; Foundational experience in security detection/prevention technology to include intrusion detection (network based & host based); intrusion prevention; deep packet inspection; anomaly detection; behavioral based detection; and wireless detection;

Foundational experience in using IDS Software and/or ePO log checks to monitor networks and/or operating systems to track network events and activities and report all incidents to appropriate personnel; Basic knowledge of threat definitions used to identify anomalous network behavior or traffic patterns against steady-state, baseline network activity; Foundational experience in using packet capture tools to examine data from live networks and identify potential anomalies; Foundational experience with network security such as Access Control List; IPSec & SSL based virtual private network technology; remote access; Firewalls (stateful packet inspection, application level); and application acceleration technologies. **Note: The contents of your resume must fully and explicitly support this response in its entirety. Otherwise, you will be found ineligible.**

OR

Currently enrolled in a Bachelor's or equivalent undergraduate degree. Bachelor's or master's degree program in an accredited university with a major in Computer Science, Electrical Engineering, Electronics Engineering, Computer Engineering, Network Engineering, Software Engineering, Supply Chain, Information Assurance, Information Technology, Systems Research, Systems Applications, Information Systems, Information Security, Software Assurance, Management Information Systems (MIS), Network & Systems Administration, Computer Information Systems Management, Information Systems Security, Information Security Management, Information Security Institute, Cybersecurity, Management and Systems, Systems Engineering, Cybersecurity and Leadership or Business with a specific concentration in one of the above; or have 15 semester hours in a combination of Mathematics, Statistics, and Computer Science.

(SUBMIT TRANSCRIPTS)

To qualify for this position at the GS-11 level, you must have the following:

Extended experience in conducting analysis of digital media images, and using tools and techniques to scan systems (e.g. work stations and servers, document and collect system state information (running processes, network connections, etc.), and documenting, collecting, and preserving digital media in the form of forensic images; Extended experience in participating in digital forensics operations for incident response; using hashing algorithms to validate forensic images; and conducting analysis on forensic images and other available evidence to draft preliminary forensic reports; Intermediate knowledge of encryption; file systems; networks; routers; servers; and various operating systems; extended experience in accessing, assessing, and gathering evidence from electronic devices using various forensic tool suites; Extended experience in using packet capture tools to examine data from live networks and identify potential anomalies; Extended experience in dynamic analysis, identifying network intrusions and using network monitoring tools to capture real-time traffic spawned by any running malicious code; identifying internet activity that is triggered by malware; Extended experience in security detection/prevention technology to include intrusion detection (network based and host based); intrusion prevention; deep packet inspection; anomaly detection; behavioral based detection; and wireless detection; Intermediate knowledge of network traffic analysis methods; threat identification; and monitoring external data sources to maintain current CND threat condition and determining which security issues may have an impact on the network or enclave;

Foundational experience in performing network monitoring and using SEIM tools, and participating in receipt and analysis of network alerts from sources possessing a high probability of system compromise to assist CND response teams in identifying malicious activities within monitored enclaves and develop draft mitigation recommendations; Foundational experience in network security such as Access Control List; IPSec & SSL based virtual private network technology; remote access; Firewalls (stateful packet inspection, application level); and application acceleration technologies. **Note: The contents of your resume must fully and explicitly support this response in its entirety. Otherwise, you will be found ineligible.**

OR

Currently Enrolled in a Master's or equivalent graduate degree. Master's degree program in an accredited university with a major in Computer Science, Electrical Engineering, Electronics Engineering, Computer Engineering, Network Engineering, Software Engineering, Supply Chain, Information Assurance, Information Technology, Systems Research, Systems Applications, Information Systems, Information Security, Software Assurance, Management Information Systems (MIS), Network & Systems Administration, Computer Information Systems Management, Information Systems Security, Information Security Management, Information Security Institute, Cybersecurity, Management and Systems, Systems Engineering, Cybersecurity and Leadership or Business with a specific concentration in one of the above; or have 15 semester hours in a combination of Mathematics, Statistics, and Computer Science. **(SUBMIT TRANSCRIPTS)**

To qualify for this position at the GS-12 level, you must have the following:

At least one full year of specialized experience comparable in scope and responsibility to the GS-11 level in the Federal service (obtained in either the public or private sectors). This experience must include activities such as: 1) implement security requirements across information technology disciplines to meet regulations; 2) assess new systems design methodologies to improve software quality; 3) identify need for changes based on new security technologies or threats; and 4) evaluate security incident response policies for potential security risks. **Note: The contents of your resume must fully and explicitly support this response in its entirety. Otherwise, you will be found ineligible.**

In addition to meeting the minimum qualifications above, you must meet the following competencies:

1. Attention to Detail - Is thorough when performing work and conscientious about attending to detail.
2. Customer Service - Works with clients and customers (that is, any individuals who use or receive the services or products that your work unit produces, including the general public, individuals who work in the agency, other agencies, or organizations outside the Government) to assess their needs, provide information or assistance, resolve their problems, or satisfy their expectations; knows about available products and services; is committed to providing quality products and services.
3. Oral Communication - Expresses information (for example, ideas or facts) to individuals or groups effectively, taking into account the audience and nature of the information (for example, technical, sensitive, controversial); makes clear and convincing oral presentations; listens to others, attends to nonverbal cues, and responds appropriately.

4. Problem Solving - Identifies problems; determines accuracy and relevance of information; uses sound judgment to generate and evaluate alternatives, and to make recommendations.

Education:

For any college courses, graduate work, research, thesis or other non-descript courses listed on your transcript (such as "Independent Research"), please indicate through your resume or attachment memorandum from an academic professor how each course fulfills the specific education requirement, i.e., state number of semester hours credited, topic of study, grade earned. Currently Enrolled in a Master's or equivalent graduate degree. Master's degree program in an accredited university with a major in Computer Science, Electrical Engineering, Electronics Engineering, Computer Engineering, Network Engineering, Software Engineering, Supply Chain, Information Assurance, Information Technology, Systems Research, Systems Applications, Information Systems, Information Security, Software Assurance, Management Information Systems (MIS), Network & Systems Administration, Computer Information Systems Management, Information Systems Security, Information Security Management, Information Security Institute, Cybersecurity, Management and Systems, Systems Engineering, Cybersecurity and Leadership or Business with a specific concentration in one of the above; or have 15 semester hours in a combination of Mathematics, Statistics, and Computer Science.

(SUBMIT TRANSCRIPTS)

NOTE: Education must be accredited by an accrediting institution recognized by the U.S. Department of Education in order for it to be credited towards qualifications (particularly positions with a positive education requirement). Applicants can verify accreditation at the following website:

<http://ope.ed.gov/accreditation/search.aspx>. All education claimed by applicants will be verified by the appointing agency accordingly.

Special Instructions For Foreign Education: If you are using education completed in foreign colleges or universities to meet the qualification requirements, you must show that the education credentials have been evaluated by a private organization that specializes in interpretation of foreign education programs and such education has been deemed equivalent to that gained in an accredited U.S. education program; or full credit has been given for the courses at a U.S. accredited college or university. For further information, visit: <http://www.ed.gov/about/offices/list/ous/international/usnei/us/edlite-visitus-forrecog.html>

New employees must serve a one year probationary period.

This position may require shift work on a 24x7x365 basis and incumbent may be required to work weekends, nights and/or holidays on a rotational basis or as the need/workload dictates.

This position may be designated as essential personnel. Essential personnel must be able to serve during continuity of operation events without regard to declarations of liberal leave or government closures due to weather, protests, acts of terrorism, or lack of funding.

Failure to report for or remain in this position may result in disciplinary or adverse action in accordance with applicable laws, rules, and regulations (5 U.S.C. § 7501-7533 and 5 CFR Part 752, as applicable).

HOW YOU WILL BE EVALUATED:

Once the application process is complete, a review of resume and supporting documentation will be made to determine if you are qualified for this job. If, after reviewing your resume and/or supporting documentation, a determination is made that you have inflated your qualifications and/or experience, you may lose consideration for this position. Please follow all instructions carefully. Errors or omissions may affect your eligibility.

Your qualifications will be evaluated on the following competencies (knowledge, skills, abilities and other characteristics):

- KNOWLEDGE OF IT SECURITY PRINCIPLES, CONCEPTS, AND METHODS
- KNOWLEDGE OF PROJECT AND PROGRAM MANAGEMENT PRINCIPLES, METHODS AND PRACTICES
- ABILITY TO EVALUATE THE EFFECTIVENESS OF IT SECURITY PROGRAMS

Applicants will be evaluated on their total background including experience (paid and unpaid), education, awards, and training and self-development as it relates to the position based upon the information provided in the resume/application and any other supporting documents. If you are a current or former Federal employee, your resume must indicate the GS or pay band level for each position that you held. If your resume includes non-government service, including contractors, please include the salaries for each position held. All work experience should specify the length of time spent in the position. One year of specialized experience is equivalent to 12 months at 40 hours per week. Part-time hours are prorated.

Please note: If a determination is made that you have rated yourself higher than is apparent in your description of experience and/or education OR that your application is incomplete, you will be rated ineligible or your score may be lowered.

Evaluation of Experience: Please include ALL applicable work experience that relates to the position for which you are applying. You must include months and years to receive credit for your work experience. You may use additional sheets to describe your work experience. One year of specialized experience is equivalent to 12 months at 40 hours per week. Part-time hours are prorated. You will not receive any credit for experience that indicates hours per week "varies." List exact hours per week on each job experience.

Application of Veterans' Preference: Category rating and selection procedures place those with veteran's preference above non-preference eligible within each category.

Veterans who meet the eligibility and qualification requirements **and** who have a compensable service-connected disability of at least 10 percent are listed in the highest quality category, except when the position being filled is scientific or professional at the GS-09 grade level or higher.

BENEFITS:

The Federal Government offers a comprehensive benefits package. Explore the major benefits offered to most Federal employees at

<http://www.opm.gov/healthcare-insurance/>

OTHER INFORMATION:

Promotion Potential: This position has promotion potential to GS- 12.

Background Investigation: To ensure the accomplishment of our mission, DHS requires every employee to be reliable and trustworthy. To meet those standards, all selected applicants must undergo and successfully pass a background investigation for Suitability, Secret, Top Secret or Top Secret/SCI clearance as a condition of placement into this position. Continued employment is contingent upon favorable adjudication of periodic reinvestigations.

Other Information:

This position has been designated exempt from bargaining unit representation under the national security provision of 5 USC Section 7112(B)(6).

All employees are required to participate in Direct Deposit/ Electronic Funds Transfer for salary payments.

If you are a male born after December 31, 1959, and are at least 18 years of age, civil service employment (5 U.S.C. 3328) requires that you must be registered with the Selective Service System, unless you meet certain exemptions under Selective Service law. If you are required to register but knowingly and willfully fail to do so, you are ineligible for appointment by executive agencies of the Federal Government.

HOW TO CLAIM VETERANS PREFERENCE (FedshireVets.gov):

If you are a *Discharged, Non-Disabled Veteran*, you must submit a copy of your DD-214 showing character of discharge (Member 4 copy), or other Documentation of Service and Separation under Honorable Conditions, as listed on the [SF15](#). If you don't have your DD-214, you may request it after discharge from the National Archives at www.archives.gov/veterans

If you are a *veteran within 120 days of discharge*, you must submit signed documentation from the Armed Forces certifying: 1) your expected release/retirement from active duty, 2) under honorable conditions, 3) your pay grade/rank/rate at time of discharge, 4) dates of active duty service, 5) any

campaign or expeditionary medals received, 6) dated within 120 days of your separation. If you are a Disabled Veteran, Purple Heart Recipient, or Mother or Spouse of a Disabled or Deceased Veteran, you must submit all additional proof required by the SF15, and if applicable, a completed SF15. If you don't have your Department of Veterans Affairs letter establishing proof of disability, you may request it at <http://www.ebenefits.va.gov/> or call 1-800-827-1000.

HOW TO APPLY:

To apply for this position, you must provide a complete Application Package which includes:

1. Your **Résumé** and other **supporting documents** specified in the **Required Documents** section below.
2. A copy of your college transcripts (Undergraduate and/or Graduate)

A complete Application Package must be received by 11:59 PM, Eastern Time, on the closing date of Monday, January 19, 2015.

*To begin the process, send your application package via email to the following mailbox:
NPPDJobApplications@hq.dhs.gov

*The subject line of the email MUST state the following Vacancy ID: **ScdA-CYB003-CS-15**

APPLICATIONS WILL ONLY BE ACCEPTED VIA EMAIL AND MUST FOLLOW THE PROCESS EXPLAINED IN THE **"HOW TO APPLY SECTION"** IN ORDER TO RECEIVE CONSIDERATION.

REQUIRED DOCUMENTS:

The following documents are required and must be received by the closing date of this announcement:

1. Your **Résumé**
2. Other **Supporting Documents**:
 - Veterans Preference Documentation, if applicable
 - SF-50, Notification of Personnel Action (if applying as a status candidate with current or former Federal service)
 - Transcripts (if qualifying based on education) or list of college courses with credits, major(s) and grade point average or class ranking. (Unofficial or photocopies are acceptable at time of application. Official transcript(s) will be required prior to appointment if you are selected.)

Current or former Federal employees **MUST** submit a copy of their SF-50 Form which shows competitive service appointment, tenure group, grade, and salary. If you are applying for a higher grade, please provide the SF-50 Form which shows the length of time you have been in your current/highest grade (examples of appropriate SF50s include promotions, With-in Grade/Range Increases, and SF-50s over one year old).

If you have promotion potential in your current position, please provide proof. Employees applying with an interchange agreement must provide proof of their permanent appointment. *IF YOU DO NOT SUBMIT ALL OF THE REQUIRED DOCUMENTATION, YOU WILL NOT RECEIVE CONSIDERATION AS A STATUS CANDIDATE.*

AGENCY CONTACT INFO:

Cathy Stokes

NPPDJobApplications@hq.dhs.gov

Tel. (703) 235-2105

1616 Ft. Myer Dr.

Arlington, VA 22209

WHAT TO EXPECT NEXT:

Once the complete application package email is received, you will be notified via email that your submission was successful. Based upon your qualifications, you may be referred to the hiring official. If your name is referred to the hiring official, you may be contacted directly by that office for a possible interview.

You will receive notice via the email provided by you during the application process, once this process is completed (generally 4-6 weeks).

[EEO](#) | [Reasonable Accommodations](#) | [Veterans Information](#) | [Privacy Policy Guidance](#) | [FOIA](#)