Content Analysis of Job Advertisements

Jeggo Paolo V. DyCok

Professor Lafever

September 30, 2023

Job advertising are crucial in determining the expectations and prospects for job searchers in the ever-changing work market. In order to identify the underlying trends, subtleties, and signals that these job advertising represent to prospective candidates, this content analysis dives deeply into the minute aspects of job advertisements in the field of cybersecurity. By definition, "Content Analysis is a qualitative analysis method that focuses on analyzing communication taken from primary and secondary data or artifacts" (Lafever, 2023). In this study, content analysis is used to examine a wide range of cybersecurity job postings from various industries. This project is important because it has the ability to shed light on the variable nature of cybersecurity employment, the particular skills and certifications that are in demand, and the preferences of cybersecurity employers. All of this information can greatly benefit job seekers, helping them navigate the cybersecurity job market more effectively. This paper explores several major points related to cybersecurity job advertisements, including the use of language and tone, the presentation of job requirements, and the depiction of company culture and values in this specialized field. Shedding light into these aspects aim to contribute to a deeper understanding of the dynamics between employers and job seekers in the contemporary cybersecurity job market. Subsequently, this paper discusses the implications of the research findings and their potential impact on job-seeking strategies within the cybersecurity sector.

I am actively exploring diverse and exciting career opportunities within the realms of Cybersecurity, Information Technology, and System Administration, with a keen focus on positions that align with my qualifications, skills, and career aspirations. Let's delve into the specifics of the four distinct roles that have captured my interest.

Firstly, within the Department of Homeland Security's Cybersecurity Service, I am intrigued by the prospect of a Cybersecurity Threat Analysis role. This encompasses positions such as Cybersecurity Threat Analyst, Cybersecurity Threat Intelligence Analyst, or Cybersecurity Defense Operations Analyst. The responsibilities associated with this position include the collection, processing, and analysis of cyber warning assessments. With a minimum of three years of cybersecurity work experience, I am well-positioned to contribute effectively to this role. While the job advertisement doesn't explicitly mention remote work or detailed benefits, the structured assessment process and the critical national security mission of the DHS align with my preference for a methodical and impactful career in government cybersecurity. Next, in the realm of Information Technology, I am considering an Information Engineer position at CACI. This role involves the management of software licenses, validation of software manufacturer information, and addressing customer inquiries related to software licensing. The job posting emphasizes proficiency in Microsoft Office applications and Unix experience as beneficial, making it clear that these are skills I am open to acquiring during the training period. The role is on-site, and CACI's reputation as a Best Place to Work, coupled with its character-based culture and mission-oriented approach, resonates with my values and career preferences. Moving on to the Linux Systems Administrator role at CACI, this position intrigues me with its multifaceted responsibilities. It entails maintaining the smooth operation of multi-user computer systems, coordinating with network administrators, and evaluating vendor products. While the extensive ten years of System Administration experience may initially seem daunting, I am eager to undergo the necessary training to meet these expectations. The role not only involves hardware and software management but also includes responsibilities such as system

documentation, performance tuning, and network configuration, aligning well with my skills and interests in Information Technology. Lastly, within the Department of Energy's Office of Environmental Management - Savannah River Operations Office, I am exploring the Information Technology Cybersecurity Specialist position. This role emphasizes ensuring security compliance and achieving/maintaining Authority to Operate (ATO) for IT and Operational Technology systems. It involves serving as a lead for cybersecurity projects, demonstrating competencies in attention to detail, customer service, oral communication, and problem-solving. The position is open to various applicant categories, underlining its inclusive nature, and offers an opportunity to contribute to cybersecurity within the Department of Energy.

Content Analysis

The roles of Cybersecurity Threat Analysis, Network Engineer, Linux System Administrator, and Information Technology Cybersecurity Specialist contain common themes and patterns that have been discovered by a thorough analysis of the offered job descriptions. It's important to keep in mind that employment advertisements could show an idealized future state rather than the actual situation of the job market at the time (Harper, 2012). This emphasizes the concept that job descriptions frequently present an idealized view of the employment, particularly in government posts when experience at a particular paygrade is mentioned. Companies often avoid talking about salary for salaried roles when discussing salary. compensation terms like "competitive salary" and "salary commensurate with experience" are frequently used yet provide little insight. According to Burry (2022), "businesses often are cautious when it comes to paid employees. The words "salary commensurate with experience" or "competitive salary" are examples of non-revealing language that a candidate may encounter. This implies that there could be some opportunity for bargaining depending on the applicant's

credentials and expertise. The position of Cybersecurity Threat Analysis, when broken down into its component job categories, largely entails obtaining, evaluating, and distributing cyber threat assessments and has a minimum requirement of three years of cybersecurity expertise. Although particular skills are not expressly listed, the focus of the Network Engineer function is software licensing management, with knowledge of Microsoft Office and Unix being desirable. For the Linux System Administrator, qualifications include a bachelor's or master's degree and ten years of experience. Responsibilities include managing multi-user systems, documenting systems, and configuring networks. As a result, the Information Technology Cybersecurity Specialist function demands specialized knowledge at the GS-12 level and places a significant focus on cybersecurity leadership, compliance, and awareness. These findings clarified the complex nature of job postings, which frequently portray an idealized perspective of occupations. As a result, it is vital for job searchers to assess their qualifications against these standards.

Conclusion

In conclusion, the analysis of job advertisements within the cybersecurity field reveals not only the specific requirements and responsibilities associated with various roles but also the nuances and subtleties embedded within these postings. This content analysis has shed light on the dynamic nature of cybersecurity employment, emphasizing the importance of understanding the language, tone, and implied expectations within job listings. Job seekers can benefit greatly from this insight, as it equips them with the knowledge to navigate the ever-evolving cybersecurity job market more effectively. By uncovering common patterns and highlighting the potential discrepancies between idealized job descriptions and actual market conditions, this research provides valuable guidance for those pursuing careers in this specialized field. Ultimately, this study contributes to a deeper understanding of the intricate relationship between

employers and job seekers in the contemporary cybersecurity job market, offering meaningful insights that can inform strategic decision-making in job searches and negotiations.

References

Burry, M. (2022, February 1). *How to Decipher a Job Advertisement*. Retrieved from The Balance: https://www.thebalancemoney.com/how-to-decode-a-job-advertisement-2061002

CACI, (2023). Information Engineer. CACI careers.

CACI, (2023). Linux System Administrator. CACI careers.

Department of Homeland Security (2023, September). Cybersecurity Threat Analysis – Developmental. USAJOBS.

Harper, R. (2012). The collection and analysis of job advertisements: a review of research methodology. In R. Harper, The collection and analysis of job advertisements: a review of research methodology (p. 30).

Lafever, K. (2023). Content Analysis. Norfolk; Old Dominion University.

Office of Environmental Management – Savannah River Operations Office, Department of Energy. (2023, September). Information Technology Cybersecurity Specialist. USAJOBS

Job #1

Link: https://www.usajobs.gov/job/750058900

Summary

The Department of Homeland Security (DHS) is recruiting professionals to support a range of developmental roles in Cybersecurity Threat Analysis, including Cybersecurity Threat Analyst, Cybersecurity Threat Intelligence Analyst, and Cybersecurity Defense Operations Analyst. All positions are in the DHS Cybersecurity Service.

This job is open to

The public

U.S. Citizens, Nationals or those who owe allegiance to the U.S.

Duties

There are a variety of Cybersecurity Threat Analysis opportunities across the Department, including supporting several specialized programs at the Cybersecurity and Infrastructure Security Agency (CISA), DHS Office of the Chief Information Officer (OCIO), and the Federal Emergency Management Agency (FEMA.

As a DHS Cybersecurity Service employee in the Developmental Career Track, you will continually and proactively participate in learning activities to enhance and apply your developing expertise in the technical capability of Cybersecurity Threat Analysis to perform a range of routine tasks, which may include:

- Collecting, processing, analyzing, and disseminating cyber warning assessments.

- Applying knowledge of cybersecurity threats to determine possible consequences to DHS and draft or recommend mitigation strategies.
- Performing code analysis, traffic analysis, web log analysis, and pattern analysis to determine possible trends, patterns, and suspicious activity on networks.
- Tracking technical network and host-based attack vectors, malicious actors, emerging cyber threats, new vulnerabilities, and current trends to prepare and present cyber threat intelligence briefings to DHS leadership.
- Actively participating in Departmental, Component, or Federal working groups, task forces, and committees to develop, share or otherwise contextualize cyber indicators or information, recommending countermeasure or mitigation strategies for perceived threats.
- Applying Intelligence Community (IC) standards to analyze all-source intelligence on current and emerging cyber threats and sharing this analyses with DHS customers and partners.
- Producing routine intelligence assessments and cyber warning assessments to identify and evaluate emerging threats.
- Monitoring DHS or Component architectures, networks, communications, applications, and systems by mining open source and classified data sources.
- Actively working with Cyber Incident Response teams and cyber experts to implement identification and protection measures against state sponsored threats, sharing intelligence and analysis.
- Performing routine scanning and probing activities to analyze and interpret all-source intelligence on current and emerging cyber threats using intelligence community analytical standards.

Requirements

Conditions of Employment

- You must be a U.S. Citizen or national.
- You must be 18 years of age.
- Must be registered for the Selective Service (if you are a male).
- Must be able to obtain and maintain a security clearance. Security clearance levels may vary.
- Must be able to submit to a drug test and receive a negative result.
- Must be able to comply with ethics and standards of conduct requirements, including completing any applicable financial disclosure.
- May be required to serve a 3 year probationary period.
- While many of these positions are considered telework eligible, some individuals must live within 2 hours driving distance to a DHS SCIF in either Chandler, AZ; Stennis, MS; Idaho Falls, ID; Arlington, VA; Pensacola, FL; Springfield, VA or D.C.
- Remote work may be available for some positions.

Qualifications

This position is in the Developmental Track at the Associate Cybersecurity Specialist career level. At this level, individuals generally:

- Have 3+ years of cybersecurity work experience
-

- Can serve as a cybersecurity professional with some experience who applies still-burgeoning technical expertise to perform routine work with significant supervision and clear guidance.

DHS Cybersecurity Service employees with a technical capability in Cybersecurity Threat Analysis will generally:

- Collect, analyze, and report on cybersecurity threats and threat actors to support operations.
- Understand and analyze different sources of information (e.g., INTs, open source, law enforcement data) on specific topics or targets.
- Provide tactical/operational analysis, including attribution of cyber actors using a variety of analytic techniques and tools. May also provide strategic-level analysis to support broader mission.
-
- Develop and communicate situational awareness of local, regional, and international cybersecurity threats impacting stakeholder missions and interests.

DHS Cybersecurity Service employees start at career levels and salaries matching their experience and expertise. To learn more about DHS Cybersecurity Service career tracks and levels, visit our application portal.

This position is focused on Cybersecurity Threat Analysis.

DHS Cybersecurity Service jobs are structured cybersecurity specializations - called technical capabilities. To learn more about technical capabilities, visit our application portal.

Education

Degrees are not required for jobs in the DHS Cybersecurity Service, but DHS is interested in your level of education and the topics you studied. As you submit initial application information, you will be asked questions about your education.

Additional information

Salary: Listed salary ranges reflects typical starting salaries available to employees in most of the United States across applicable career levels. In some geographic areas, average starting salaries will be higher because of a local cybersecurity labor market supplement (e.g., metro Washington, D.C. +10%). Actual salaries of individual employees may be higher or lower than provided figures. For an overview of the salaries available in the DHS Cybersecurity Service, visit Resources.

Benefits: DHS Cybersecurity Service employees receive a range of federal employment benefits designed to support their professional and personal lives. To learn more about benefits, visit our application portal.

More information about the specific benefits available to you will be provided as you progress through the application process.

Background Investigation: To ensure the accomplishment of its mission, the Department of Homeland Security (DHS) requires each and every employee to be reliable and trustworthy. To meet those standards, all selected applicants must undergo and successfully complete a background investigation for a security clearance as a condition of placement in this position.

This review includes financial issues such as delinquency in the payment of debts, child support and/or tax obligations, as well as certain criminal offenses and illegal use or possession of drugs.

Pursuant to Executive Order 12564 and DHS policy, DHS is committed to maintaining a drug-free workplace and, therefore, conducts random and other drug testing of its employees in order to ensure a safe and healthy work environment. Headquarters personnel in safety- or security-sensitive positions are subject to random drug testing and all applicants tentatively selected for employment at DHS Headquarters are subject to drug testing resulting in a negative test result.

Benefits

A career with the U.S. government provides employees with a comprehensive benefits package. As a federal employee, you and your family will have access to a range of benefits that are designed to make your federal career very rewarding. Opens in a new windowLearn more about federal benefits.

Eligibility for benefits depends on the type of position you hold and whether your position is full-time, part-time or intermittent. Contact the hiring agency for more information on the specific benefits offered.

How You Will Be Evaluated

You will be evaluated for this job based on how well you meet the qualifications above.

All DHS Cybersecurity Service applicants participate in a multi-phase assessment process, which varies by career track. For the Developmental Career Track, applicants participate in a two-phase assessment process:

- You must successfully complete each phase to advance to the next phase.
- The total time commitment for the two phases is approximately 3 hours (many applicants require less time!)
- Before each phase, DHS will e-mail you instructions and information to help you prepare.
- Monitor your e-mail to ensure you have plenty of time to complete assessments prior to any deadlines or request an extension, if necessary

PHASE I: ONLINE ASSESSMENTS

- Unproctored - you choose the time and location
- Includes two assessments: (1) a work styles inventory that will take about 30 minutes to complete; (2) a work simulation that you will have up to 2 hours to complete.
- The two assessments take about 90 minutes (on average) to complete.
- Requires a computer with audio (speakers or headphones) and a reliable internet connection.
- No knowledge of DHS or cybersecurity is required for these assessments, which measure non-technical capabilities that are important for professional success in the DHS Cybersecurity Service. This includes how you communicate, analyze information, and collaborate with others:
- The work styles inventory presents you with questions about your work-related interests and preferences.

- The work simulation presents you with realistic, work-related scenarios and asks you to respond to them.

PHASE II: TECHNICAL CAPABILITY ASSESSMENT

- Proctored - must be scheduled in advance and completed at a designated assessment center.
-
- There is a different assessment for each DHS Cybersecurity Service technical capability (visit Jobs to learn more about the technical capabilities).
-
- Most individuals only have a primary technical capability and complete only one Technical Capability Assessment, but in limited circumstances, you may complete a second Technical Capability Assessment.
-
- You will have up to 2.5 hours to complete each Technical Capability Assessment; each takes about 90 minutes (on average) to complete.
-
- Assessments present realistic, work-related cybersecurity scenarios and questions to assess technical skills.
-
- Cybersecurity knowledge **is** assessed, but no knowledge of DHS is required.

Your un-proctored and proctored assessment results are valid for a period of one year after completion and will be kept and used toward future positions for which you might apply that

require the same assessments.

To learn about the assessment process for this Developmental Track position, visit our portal and read the "Assessment Process" guide.

Required Documents

1. Your resume. To help you prepare your resume before applying to the DHS Cybersecurity Service, visit our application portal and read the "Resume Tips" guide.
2.
3. If you are requesting a reasonable accommodation to the online assessments, submit documentation to support your request, including the Reasonable Accommodation Request Form found here.
4.
5. If you are a current or former political Schedule A, Schedule C, Non-career SES or Presidential Appointee employee please submit a copy of your applicable SF-50, along with a statement that provides the following information regarding your most recent political appointment:- Position title- Type of appointment (Schedule A, Schedule C, Non-career SES, or Presidential Appointee)- Agency- Beginning and ending dates of appointment

How to Apply

To apply for this position, you must complete the initial online questionnaire, required assessments, and submit the documentation specified in the Required Documents section below.

The complete application package must be submitted by 11:59 PM (ET) on 10/20/2023 to receive consideration. The application process will follow the bullets outlined below.

6. To begin the application process, click the Apply Online button.
7.
8. Answer the questions presented in the application and attach all necessary supporting documentation.
9. Click the Submit Application button prior to 11:59PM (ET) on the announcement closing date.
10. After submitting an online application, you will be notified whether or not you are required to take additional online assessments through the USA HIRE platform. This message will be delivered via email notification.
11. If you are asked to take the online assessments, you will be presented with a unique URL to access the USA Hire system. Access to USA Hire is granted through your USAJOBS login credentials.

Be sure to review all instructions prior to beginning online assessments. Note: set aside at least 3 hours to take these assessments; however, most applicants complete the assessments in less time. If you need to stop the assessments and continue at a later time, you can re-use the URL sent to you via email and also found on the Additional Application Information page that can be located in the application record in your USAJOBS account.

Reasonable Accommodation Requests: If you believe you have a disability (i.e., physical or mental), covered by the Rehabilitation Act of 1973 as amended and Americans with Disabilities

Act 1990 as amended, that would interfere with completing online assessments on the USA HIRE platform, you will be granted the opportunity to request a reasonable accommodation in your online application. Requests for Reasonable Accommodations for the USA Hire Competency Based Assessments and appropriate supporting documentation for Reasonable Accommodation must be received prior to starting the online assessments. Decisions on requests for Reasonable Accommodations are made on a case-by-case basis. If you meet the minimum qualifications of the position, after notification of the adjudication of your request, you will receive an email invitation to complete the online assessments. You must complete all assessments within 48 hours of receiving the URL to access the online assessments. To determine if you need a Reasonable Accommodation, please review the Procedures for Requesting a Reasonable Accommodation for online assessments here: http://help.usastaffing.gov/Apply/index.php?title=Reasonable_Accommodations_for_USA_Hire.

Agency contact information

DHS Cybersecurity Service Talent Team

Email

cybersecurityservice@hq.dhs.gov

Address

Cybersecurity Talent Management System

245 Murray Lane SW

Washington, DC 20528

US

Learn more about this agency

Next steps

The DHS Cybersecurity Service application process is designed to both prioritize fairness to all applicants and identify qualified candidates to join the DHS Cybersecurity Service. Successful applicants proceed through the following steps and will receive notifications as each step is completed: Submit Initial Information

- Upload resume
- Answer questions about your expertise and experience

Assessment + Interview

- Complete multi-phase assessment process
- Interview with the team you might join

Tentative Job Offer + Background Investigation

- Receive a tentative job offer, including your compensation and benefits package
- Receive an invitation to start the background investigation process

Final Job Offer + Start Date

- Receive a final job offer
- Determine your start date

We will notify you by email after each of these steps has been completed. Your status will also be updated on USAJOBS throughout the process. To check your status, log on to your USAJOBS account, click on "Application Status," and then click "More Information."

Note: If you successfully complete the application process and receive a tentative DHS Cybersecurity Service job offer, applicable employment eligibility requirements, including those you must comply with throughout your appointment at DHS, will be communicated to you in writing.

Any offers of employment made pursuant to this announcement will be consistent with all applicable authorities, including Presidential Memoranda, Executive Orders, interpretive U. S. Office of Management and Budget (OMB) and U. S. Office of Personnel Management (OPM) guidance, and Office of Management and Budget plans and policies concerning hiring. These authorities are subject to change.

DHS uses e-Verify, an Internet-based system, to confirm the eligibility of all newly hired employees to work in the United States. Learn more about E-Verify, including your rights and responsibilities.(http://www.uscis.gov/e-verify).

To learn more about DHS Cybersecurity Service employment eligibility, visit our application portal.

Job #2:

Link: https://careers.caci.com/global/en/job/282235/Information-Engineer

Information Engineer

Job Category: Information Technology

Time Type: Full time

Minimum Clearance Required to Start: TS/SCI with Polygraph

Employee Type: Regular

Percentage of Travel Required: None

Type of Travel:

What You'll Get to Do:

- Issue, allocate and verify license entitlements for software products.
- Verify and validate software manufacturer, name, and version information.
- Review all software licensing agreements for software download from the internet.
- Create, update and edit Software Model Records.
- Perform software importation on commercial non-DoD systems.
- Address and respond to customer questions related to software licensing.
- Enforcement of Policy 6-10, Software Asset Management.

You'll Bring These Qualifications:

- Must meet contract level requirements for appropriate position.
- 1 year of experience with background in Microsoft Office applications to include Outlook, Word, and Excel is a plus.
- Experience in ticket management system like Remedy is a plus.
- Unix experience is not required but is a plus.
- Candidate MUST complete training during the first several months on contract.

(No DoD 8570 Certification Required for this Opening!)

(CCAs MAY APPLY FOR THIS OPENING.)

What We Can Offer You:

- We've been named a Best Place to Work by the Washington Post.

- Our employees value the flexibility at CACI that allows them to balance quality work and their personal lives.

- We offer competitive benefits and learning and development opportunities.

- We are mission-oriented and ever vigilant in aligning our solutions with the nation's highest priorities.

- For over 60 years, the principles of CACI's unique, character-based culture have been the driving force behind our success.

Company Overview: At CACI, you will have the opportunity to make an immediate impact by providing information solutions and services in support of national security missions and government transformation for Intelligence, Defense, and Federal Civilian customers. CACI is an Equal Opportunity/Affirmative Action Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, status as a protected veteran, or any other protected characteristic.

Job 3

Link: https://careers.caci.com/global/en/job/285532/Linux-Systems-Administrator

Linux Systems Administrator

Job Category: Information Technology

Time Type: Full time

Minimum Clearance Required to Start: TS/SCI with Polygraph

Employee Type: Regular

Percentage of Travel Required: None

Type of Travel: None

Looking for excitement, a challenge and wanting to be part of something bigger than yourself, then consider joining a winning team of professionals being assembled by CACI, Inc. We have an opening for a **Linux Systems Administrator** with an active TS/SCI w/Polygraph. If you thrive in a fast-paced and dynamic workplace, possess excellent analytic skills, and are passionate about providing mission critical support to the nation's protection and want to drive growth; we have the perfect job for you.

What You'll Get to Do:

- Maintains smooth operation of multi-user computer systems, including coordination with network administrators. Interacts with users and evaluates vendor products.
- Makes recommendations to purchase hardware and software, coordinates installation and provides backup recovery.
- Develops and monitors policies and standards for allocation related to the use of computing resources.
- Ancillary duties may include setting up administrator and service accounts, maintaining system documentation, tuning system performance, installing system wide software and allocating mass storage space.
- Configure and manage UNIX and Windows (or other applicable) operating systems and installs/loads operating system software, troubleshoot, maintain integrity of and configure network components, along with implementing operating systems enhancements to improve reliability and performance.

- Support the design of systems, mission architecture and associated hardware.
- Possess a working knowledge and understanding of system administration interdependencies as part of the Service Oriented Architecture (SOA)
- Analyze and resolve complex problems associated with server hardware, applications and software integration

You'll Bring These Qualifications:

- B.A. or B.S. degree is required.
- Ten (10) years of System Administration experience
- **Active TS/SCI Polygraph** clearance is required with Maryland Customer.

What We Can Offer You:

- We've been named a Best Place to Work by the Washington Post.
- Our employees value the flexibility at CACI that allows them to balance quality work and their personal lives.
- We offer competitive benefits and learning and development opportunities.
- We are mission-oriented and ever vigilant in aligning our solutions with the nation's highest priorities.
- For over 55 years, the principles of CACI's unique, character-based culture have been the driving force behind our success.

Company Overview: At CACI, you will have the opportunity to make an immediate impact by providing information solutions and services in support of national security missions and government transformation for Intelligence, Defense, and Federal Civilian customers. CACI is an Equal Opportunity/Affirmative Action Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation,

gender identity, national origin, disability, status as a protected veteran, or any other protected characteristic.

Job 4

Link: https://www.usajobs.gov/job/750654700

Summary

This position is part of the Office of Environmental Management - Savannah River Operations Office, Department of Energy. As an Information Technology Cybersecurity Specialist, you will work with application leads, system administrators, database administrators, developers, and testers to ensure the systems are security compliant and achieve/maintain Authority to Operate (ATO) for all Information Technology (IT) and Operational Technology (OT).

This job is open to

Career transition (CTAP, ICTAP, RPL)

Federal employees who meet the definition of a "surplus" or "displaced" employee.

Veterans

The public

U.S. Citizens, Nationals or those who owe allegiance to the U.S.

Clarification from the agency

This is a Direct Hire Public Notice. Please read this Public Notice in its entirety prior to submitting your application for consideration.

Duties

As an Information Technology Cybersecurity Specialist, you will:

- Serve as the lead for projects, tasks, working groups, and daily activities with responsibility for analyzing, managing or performing work necessary to plan, design, develop, test, implement, integrate, maintain, or modify IT systems to meet cybersecurity standards.
- Develop and maintain a high level of awareness and understanding of cybersecurity and security concerns and issues, such as the processing environment and architecture, training certification, trends, and technical problems.
- Serve as a leader or member on various standing information technology management boards, committees and working groups, as well as ad-hoc groups convened by DOE offices; Prepare and provide briefings to leadership on assigned programs and projects.
- Plan and coordinate the development and implementation of cybersecurity requirements, including serving as the lead for projects, tasks, working groups, and daily activities with responsibility for analyzing, managing, or performing work necessary to plan, design, develop, test, implement, integrate, maintain, or modify IT systems to meet cybersecurity standards.

Requirements

Conditions of Employment

- Must be a U.S. Citizen or National.
- This employer participates in the e-Verify program.
- Males born after 12/31/1959 must be registered for Selective Service.

- Subject to satisfactory security and suitability requirements.
- May be required to successfully complete a probationary period.
- This position is a Testing Designated Position (TDP) subject to applicant testing and random drug testing thereafter. Failure to test or a positive result on random drug tests conducted after appointment may result in removal from Federal employment.
- This position has been designated as Critical-Sensitive (CS)/High Risk and requires a security clearance at the DOE Q level. The incumbent is required to obtain and maintain this clearance level.
- Occasional travel may be required.
- This position is not included in a Bargaining Agreement.

Qualifications

BASIC REQUIREMENT:

For all positions, individuals must demonstrate they have experience in each of the four competencies listed below; the experience does not have to be IT-related. The employing agency is responsible for identifying the specific level of proficiency required for each competency at each grade level based on the requirements of the position being filled.

12. **Attention to Detail** - Is thorough when performing work and conscientious about attending to detail.
13. **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.

14. **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.
15. **Problem Solving** - Identifies problems; determines accuracy and relevance of information; uses sound judgment to generate and evaluate alternatives, and to make recommendations.

In addition to meeting the "Basic Requirements", you must also meet the "Specialized Experience Requirements" described below.

SPECIALIZED EXPERIENCE REQUIREMENTS: A qualified candidate's online application and resume must demonstrate at least one year of specialized experience equivalent to the GS-12 level. Specialized experience for this position is defined as meeting **ALL** of the following:

- Providing technical advice and instruction on cyber security issues; **AND**
- Participating in the collection and analysis of technical and management data associated with a cyber security program; **AND**
- Preparing various documents (reports, briefings, summaries, progress reports, etc.) pertaining to cyber security requirements

"Experience" refers to paid and unpaid experience. Examples of qualifying unpaid experience may include: volunteer work done through National Service programs (such as Peace Corps and AmeriCorps); as well as work for other community-based philanthropic and social organizations. Volunteer work helps build critical competencies, knowledge, and skills; and can provide valuable training and experience that translates directly to paid employment. You will receive credit for all qualifying experience, including volunteer experience.

CTAP/ICTAP candidates: To be considered "well qualified" you must meet all of the requirements as described in this section.

You must meet all qualifications and eligibility requirements by the closing date of this announcement.

Education

There are no specific education requirements or substitution of education for experience for this position.

Additional information

- The U.S. Department of Energy fosters a diverse and inclusive workplace and is an Equal Opportunity Employer.
-
- This job opportunity announcement may be used to fill additional similar vacancies across DOE.
- For general information on government-wide Telework polices visit: www.telework.gov

- Hiring incentives may be authorized in accordance with agency policy and if funding is available.
- EEO Policy: https://help.usajobs.gov/index.php/EEO_Policy_Statement
- Reasonable Accommodation Policy: https://help.usajobs.gov/index.php/Reasonable_Accommodation_Policy_Statement
- Veterans Information: https://help.usajobs.gov/index.php/Veterans_Information
- Selective Service Registration: http://www.sss.gov/

Benefits

A career with the U.S. government provides employees with a comprehensive benefits package. As a federal employee, you and your family will have access to a range of benefits that are designed to make your federal career very rewarding. Opens in a new windowLearn more about federal benefits.

Eligibility for benefits depends on the type of position you hold and whether your position is full-time, part-time or intermittent. Contact the hiring agency for more information on the specific benefits offered.

How You Will Be Evaluated

You will be evaluated for this job based on how well you meet the qualifications above.

You will be evaluated for this job based on how well you meet the qualifications above. This position is announced under a government-wide Direct-Hire Authority (DHA) for Information Technology Cybersecurity Specialist positions in the 2210 series. Under the DHA, applicants who meet the Education and Qualification requirements listed in this announcement will be

referred for consideration. Veteran's Preference, category rating, and traditional rating and ranking of applicants do not apply under the DHA process.

Appointments made under the DHA are processed as "new" appointments. Current Federal employees may be required to serve a new probationary period (5 CFR 315.802(b).

Successful candidates will possess the following competencies (knowledge, skills, abilities and other characteristics):

- Computer Network Defense
- Information Assurance
- Information Systems/Network Security
- Knowledge Management
- Technical Competence

Career Transition Assistance Programs: If you are eligible for career transition assistance, such as ICTAP or CTAP, you must meet the Education and Qualification requirements to be referred for consideration.

You must meet all qualifications and eligibility requirements by the closing date (10/10/2023) of this announcement.

To preview the Assessment Questionnaire, click https://apply.usastaffing.gov/ViewQuestionnaire/12132951

Required Documents

To apply for this position, you **MUST** provide a complete application package which includes:

- Your **RESUME** showing all relevant work experience (paid and unpaid) including: duties performed; full name and address of each employer; start and end dates (month/day/year); work schedule (part-time, full-time, number of hours if intermittent); salary; and any completed education and training (program title, subject area, number of hours completed, and completion date).
- **Cover Letter**, *optional*, expressing additional information not covered in your resume.
- **Transcripts,** *if specific educational requirements are indicated in this job announcement.*Unofficial transcripts or any report listing institution, course title, credits earned (semester or quarter hour) and final grade is acceptable. It is your responsibility to provide adequate proof that you meet the educational requirements.
- **Career Transition Assistance Program/Interagency Career Transition Assistance Program documentation,** *if applicable*(e.g., Certification of Expected Separation, Reduction-In-Force Separation Notice, or Notice of Proposed Removal; SF-50 that documents the RIF separation action; and most recent performance appraisal.) For more information see the OPM Guide to Career Transition.

Failure to submit any of the above mentioned required documents may result in loss of consideration due to an incomplete application package. It is your responsibility to ensure all required documents have been submitted. Do not provide photos or list a Social Security Number or date of birth on any attachment.

If you are relying on your education to meet qualification requirements:

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. Therefore, provide only the attendance and/or degrees from schools accredited by accrediting institutions recognized by the U.S. Department of Education.

Failure to provide all of the required information as stated in this vacancy announcement may result in an ineligible rating or may affect the overall rating.

How to Apply

Please read the entire announcement and all the instructions before you begin an application. To apply for this position, you must complete the initial online application, to include submission of the required documentation specified in the **Required Documents** section. A complete application package must be submitted by **11:59 PM (EST) on the announcement closing date** to receive consideration.The application process is as follows:

16. You must have a **login.gov** account to sign into USAJOBS: https://www.usajobs.gov/Help/how-to/account/.
17. To begin the application process in USAJOBS, click the **Apply Online** button.
18. Answer the questions presented in the application and attach all required and supporting documentation.
19. You must click the **Submit Application** button prior to 11:59 pm (ET) on the announcement closing date.

You may update your application, including supporting documentation, at any time during the announcement open period by returning to your USAJOBS account, select Update Application:

https://my.usajobs.gov/Account/Login. This option will no longer be available once the announcement has closed.

To verify the status of your application, during and after the announcement open period, log into your USAJOBS account; applications will appear on the Welcome screen. The Application Status will appear along with the date your application was last updated. For information on what each application status means, visit: https://www.usajobs.gov/Help/how-to/application/status/.

If you need help with login.gov or USAJOBS (e.g., account access, Resume Builder) visit the USAJOBS Help Center: https://www.usajobs.gov/Help/

If you experience difficulty applying on USAJOBS, after clicking the Apply Online button, or you are experiencing a significant hardship hindering your ability to apply online, the Agency Contact listed in the announcement can assist you during normal business hours. If you receive any system error messages, take screenshots if possible, to aid technical support.