Analyzing the Role of a Cybersecurity Analyst

Dominique J Taylor

Old Dominion University

IDS Electronic Portfolio Project

Professor Gordon-Phan

July 12, 2025

Abstract

This paper will examine the job posting for a Cybersecurity Analyst position with General Dynamics Information Technology (GDIT). The company is responsible for supporting the Naval Criminal Investigative Service (NCIS). The analysis goes over how the ad outlines key responsibilities like RMF lifecycle management, vulnerability scanning, and ATO documentation, while also reflecting both technical and implied soft skills. GDIT's job posting includes precise language and a mission-oriented tone to suggest a structured, highly trusted work environment. In this role, it comes with many challenges like maintaining compliance throughout the constant advancements within cyber threats and managing time-sensitive documentation under pressure. Using course readings from Clayton, Wright, and Nguyen, this paper will connect job ad structure and expectations to professional identity and workplace values. The paper also reflects how academic preparation, hands-on lab experience, and confidential clearance make an applicant a strong candidate.

Cybersecurity analysts are essential to protecting critical systems from evolving threats, especially within major defense environments. The cybersecurity analyst's position at General Dynamics Information Technology supports NCIS and reflects the high-stakes demands. Throughout this paper, I will analyze the job posting to show both stated qualifications and implied expectations of the position using support from Harper, Nguyen, Clayton, Zietsma, and Wright. The paper explores how job ads function as tools that reflect not only technical requirements but also workplace identity and culture. My coursework and training align closely with the position, and in this paper, I will demonstrate how academic preparation connects to real-world cybersecurity expectations.

The cybersecurity analyst position at General Dynamics Information Technology (GDIT) supports the Naval Criminal Investigative Service (NCIS), which plays a major role in protecting national security systems. GDIT, a leading government contractor that seeks professionals who can manage the "full lifecycle of RMF packages," including compliance tracking, documentation, and authorization efforts. This role requires experience with critical cybersecurity tools such as ACAS for vulnerability scanning and eMASS for maintaining security records. These technologies are standard in the Department of Defense environments, which reflects the classified and structured nature of the position. To fulfill all the responsibilities of the position, the applicant must obtain a top-secret clearance along with knowledge of NIST 800-53 controls and ATO documentation processes. This ad uses clear technical language that previews a highly disciplined work culture. Overall, the listing communicates that GDIT is looking for applicants with strong technical skills, federal security experience, and the ability to follow precise frameworks necessary to maintain secure government systems.

Although the GDIT job posting focuses heavily on technical proficiencies, a closer reading reveals several soft skills that are equally important for success within the role but isn't blatantly stated. For instance, the responsibility to "support the full lifecycle of RMF packages" implies a need for effective time management, organization skills, and the ability to multitask within strict federal compliance frameworks. Similarly, the mention of conducting vulnerability scans and using platforms such as ACAS and eMASS is an underlying statement for the need for precision and critical thinking. These tasks don't just carry a need for technical knowledge but also the ability to interpret and apply data in secure ways. Collaboration is another implied skill that, as analysts, we must have due to "coordinating with stakeholders," which implies regular interactions across departments or teams. Understanding these soft skills aligns with Harper's idea that job ads often reflect cultural expectations through task descriptions rather than direct character traits. The structured and formal tone of GDIT's ad also demonstrates a workplace culture that values discipline, clarity, and professionalism. Ultimately, while these soft skills may not be named outright, their necessity is embedded in the job responsibilities and tone that highlights the kind of well-rounded candidate the company hopes to attract.

My academic background and training in cybersecurity align with the requirements that are outlined in the GDIT's job advertisement. Taking courses in risk management, network security, and cybersecurity fundamentals has given me direct exposure to tools like Nessus and concepts like RMF and NIST 800-53 controls. Additionally, I currently hold confidential clearance, which demonstrates my trustworthiness in secure environments. Beyond technical preparation, I've developed strong communication skills through team projects, presentations, and collaborative labs, which are critical for coordinating with stakeholders. GDIT uses phrases like "support NCIS" and "mission-focused" to suggest that the culture is built upon accountability, structure, and national service. Compared to Nguyen and Clayton's articles,

organizations use both visual and verbal cues to communicate expectations and reinforce workplace culture, like in the GDIT job posting. As Wright states in his article “Improving Employee Selection with a Revised Resume Format,” resumes and hiring documents reflect personal qualities that matter, which, after reading Wright's article, I began to highlight in my portfolio and applications. However, this role can present challenges like maintaining system compliance in dynamic threat landscapes and ensuring timely ATO approvals under pressure. The ad’s confident and structured tone provides clear expectations that suggest a high-performing environment where applicants’ skills would be valued.

In reviewing the cybersecurity analyst position at GDIT, it’s clear that the role requires a combination of technical proficiency, attention to detail, and the ability to operate efficiently within a highly secure and collaborative environment. Through a deep understanding of the job advertisement and related course materials, this analysis shows how job postings convey not only qualifications but also deeper insights into company culture and expectations. My academic background within cybersecurity, including training in RMF and vulnerability analysis, has prepared me for such an important role. Overall, this job posting demonstrates how cybersecurity positions aren’t just technical but are deeply tied to public trust and national security.

References:

General Dynamics Information Technology. (2024). Cybersecurity Analyst – NCIS. USAJobs/IntelligenceCareers.gov. https://apply.intelligencecareers.gov/job-description/1246880

Harris, R., & Clayton, B. (2018). Editorial: the importance of skills – but which skills? International Journal of Training Research, 16(3), 195–199. https://doi.org/10.1080/14480220.2018.1576330

Wright, E. W., Domagalski, T. A., & Collins, R. (2011). Improving employee selection with a revised resume format. Business Communication Quarterly, 74(3), 272–286. https://doi.org/10.1177/1080569911413809

Nguyen, C. F. (2013). The ePortfolio as a living portal: A medium for student learning, identity, and assessment. International Journal of ePortfolio, 3(2), 135–148. http://www.theijep.com