U.S. Senate Cybersecurity Principal Specialist

Kevin M. McFarland

Old Dominion University

IDS493: Electronic Portfolio Project

Professor Dr. Sherron Gordon-Phan

January 31, 2025

Abstract

This analysis delves into the position of Cybersecurity Principal Specialist for the U.S. Senate, an opportunity that stood out as both prestigious and significant within the cybersecurity field. The role, essentially functioning as a lead Cybersecurity Threat Hunter and Penetration Tester, is responsible for proactively hunting threats, enhancing detection mechanisms, leading incident response efforts, and emulating adversary tactics to test and improve the Senate's cybersecurity defenses. Despite the role's prominence, the job description presents a unique mix of expectations and requirements that blur the lines between specialized technical tasks and leadership responsibilities, which could be misleading for prospective candidates.

Through an evaluation of the position, it is evident that critical thinking and communication are key components for success in this role. However, the job advertisement also underscores a recurring challenge in the cybersecurity industry—the disconnect between job titles, required experience levels, and the understanding of what constitutes an "entry-level" position. The analysis emphasizes how the field often suffers from contradictory expectations, especially for positions requiring extensive experience yet advertised as entry-level or vice versa, a systemic issue affecting both employers and job seekers.

In reflecting on my own qualifications, I recognize that while I may not meet the full seven to ten years of specialized experience as outlined in the advertisement, my background—especially in military leadership, policy development, and critical thinking—aligns with many of the core competencies required for the role.

Keywords: Cybersecurity, Senate, Critical Thinking

U.S. Senate Cybersecurity Principal Specialist

It must have been serendipity that led to me finding this job advertisement, as I have been looking at and applying for positions for nearly three years straight now. However it was at the time of doing this analysis assignment, that for the first time I have ever seen an advertisement for the United States Senate in my chosen field. And while I have seen cybersecurity positions for various three-letter agencies, I do not think I have come across, at least in my mind a more prestigious position than being a Cybersecurity Specialist for the U.S. Senate. The Senate is at the lofty top of our government, the culture there would be highly professional and formal akin to the military, without the uniforms but still a form of rank and file as evidenced by the Senate Sergeant at Arms and Speaker of the House positions. Whether it was convenient timing or serendipitous, prestige of this particular position is why I have chosen this job advertisement to analyze and see how I might fit into this position.

Sergeant At Arms and Cybersecurity Principal Specialist Role

The U.S. Senate Sergeant at Arms (SAA) originally known as the doorkeeper of the Senate, is considered the highest ranked law enforcement officer of the senate. This position, according to the United States Senate is, “elected by the senators, serves as the chief law enforcement and protocol officer of the United States Senate and is the executive officer responsible for a host of support services in the Senate (Senate).” Originally when Congress first convened in 1789, the Senate met behind closed doors, and so the “doorkeeper” secured the Senate Chambers. Now, since 1798, the title of SAA was added after Senate sessions were opened to the public and the role of the “doorkeeper” was expanded. Relevant to this Cybersecurity Specialist role, “The Office of the Sergeant at Arms is also responsible for enforcing all the rules of the Senate and protecting the Senate's hardware, network, and data. The

sergeant at arms provides Senate computers, equipment, and technology support services (Senate)."

Purpose and Responsibilities of the Cybersecurity Principal Specialist

In reviewing and analyzing the job advertisement for this position, we find that the role title is slightly askew of what the position really is for. The role is really that of a Lead Cybersecurity Threat Hunter and Penetration Tester, responsible for leading proactive hunts based on adversary tactics, techniques and procedures (TTPs) and evaluating anomalous activity for maliciousness. The Principal Specialist also serves as a tech lead for incident response and emulate adversary actions to test efficacy of network controls (Cybersecurity Principal Specialist #5301). The responsibilities of the role are further broken down and expounded upon as four key responsibilities considered crucial in protecting the digital assets of the Senate.

First is the Proactive Hunt, using threat intelligence or anomaly analysis, the Principal Specialist is to identify potential adversary activity on the network that may have evaded detection. Using the result of these hunts, update detections or make recommendations on how to enhance the security posture of the Senates digital systems. Second, Detection Creation, using adversary TTPs to create detections addressing gaps in the organizations threat detection posture, ensuring the protection and operation of the network, host, and cloud environments. Third is involvement in Incident Response, assisting Tier 1 and Tier 2 cybersecurity agents, as the technical lead, ensuring discovery of the entire scope of the threat penetration and compromise of the organizations systems. And fourth is Threat Emulation, the ability to emulate the activity of adversaries, ensuring the system is capable of identifying and responding to sophisticated threats to discover and mitigate and gaps in the threat detection posture (Cybersecurity Principal Specialist #5301).

Skill Requirements for Hunt Principal Specialist

With further analysis of the Cybersecurity Principal Specialist job advertisement, one of the key skills, although not directly mentioned is critical thinking skills. The Specialist must be able to identify threats, gaps in the detection posture, and have the ability to think and act like an adversary to test the efficacy of the system. Critical thinking skills will allow the Specialist to resolve complex cybersecurity issues and act as a subject matter expert across the Senate's digital domain.

While the advertisement does say they seek a candidate with basic knowledge in key areas of cybersecurity, they also list that the Specialist would have seven to ten years of experience. One of the findings of the Workforce Development Needs Survey conducted in 2018 was, "Relevant work experience is identified as the most important factor in recruiting, and enterprise and employability skills have increased in importance as a recruiting factor (Harris & Clayton)." However, the way this advertisement describes basic knowledge compared to years of experience is similar to a common problem in the cybersecurity field and industry. Job advertisements will often post as "entry level" or "junior" and require years of experience. Entry level is not three to five or seven to ten years of experience, it is basic knowledge with zero to limited experience. Thus a "Catch-22" problem is created in the industry, where to get a job you require experience, but you can only gain but so much experience without a job. A problem that has become systemic in an industry with practically zero percent unemployment. That measurement is also a misnomer as while there are zero positions unfilled, there are many candidates without employment in the field, so the definition and measure of "unemployed" does not really apply in this particular field and makes for a misleading interpretation of job availability and growth.

Communication skills are specifically mentioned in the job advertisement, having the ability to both verbally and in writing communicate with various audiences at varying technical levels of understanding. The communication skills also help ensure strong leadership, managing project teams and coordinating efforts across multiple departments. The ability to communicate in writing is further important as the ability to, "…develop and implement strategic cybersecurity policies, standards, and frameworks that align with the organization goals (Cybersecurity Principal Specialist #5301)."

Do I Have the Chops (Skills)

There is a level of disappointment that comes with reading and analyzing this job advertisement and seeing how I might qualify for the role. One such disappointment is in many of the misleading factors. The Cybersecurity Principal Specialist does not sound or read like a very specific role, more generalized. However, when you dive into the analysis of the advertisement, you find that the responsibilities range between being a threat hunter to being a team leader, while neither of those necessarily must be exclusive jobs, typically managing a team and focus on specific role-based skills are often separated by different roles. For example, in the United States Navy, and a Firecontrolman Chief Petty Officer, I have a background of course in weapons systems, electronics and ordnance, however as a Chief, my role is that of a personnel and program manager. I am no longer hand-on in the gear, I am leading those who are hands-on and ensuring the safe and legal operation of everything is maintained. As I have plenty of experience managing a team, I am able to communicate effectively and also have experience from the Navy developing and implementing policy and standards. Additionally, one of my courses here at Old Dominion University would also have me prepared to ensure policy and standards are maintained, CYSE525W Cyber Strategy and Policy, where I spent a semester

analyzing the National Institute of Standards and Technology Risk Management Framework, of which, by Executive Order, is mandatory for all Federal Agencies.

Do I require basic knowledge or seven to ten years of cybersecurity experience? I do not have seven to ten years of specific cybersecurity experience, but I certainly have an entry level basic knowledge and understanding of cybersecurity principals, maybe a bit more with my military service background. I do also have experience with similar systems and policies due to my internship at the Navy Exchange Headquarters. These misleading factors are a cause of disappointment as a position as prestigious as this is, one would like to think or even assume that they would rise above the industry and provide an example of how to properly define and advertise a role. As far as critical thinking skills, both my time as a student and as a member of the US Navy, I have developed, maintained and used those skills aggressively, contributing to my success so far.

Conclusion

The analysis of the job advertisement allowed to me to see that “required” years of experience and the amount of knowledge often listed in cybersecurity positions continues to be a systemic problem. It makes for a discouraging and disappointing event to hunt for jobs, one is never sure if they quite fit the bill for a job. If jobs are truly expecting years of experience for entry level knowledge and positions, it really makes it feel hopeless. There really needs to be an awakening and a re-alignment within the cybersecurity industry to manage realistic expectations and properly align skill and experience requirements to the roles.

References

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

United States Senate (2025, January 30). *Cybersecurity Principal Specialist #5301*. United States Senate. https://saa.csod.com/ux/ats/careersite/1/home/requisition/557?c=saa

United States Senate (2025, January 3). *Office of the sergeant at arms and doorkeeper*. U.S. Senate: Office of the Sergeant at Arms and Doorkeeper. https://www.senate.gov/about/officers-staff/sergeant-at-arms/sergeant-at-arms-overview.htm