

# Analysis of Cybersecurity Engineer - Technical

Jordan Sustarsic

IDS493, Professor Gordon-Phan

Old Dominion University

March 11, 2024

## Abstract

The Department of Homeland Security (DHS) is essential to protecting the US through a number of programs, one of which is cybersecurity. This analysis is focused on a particular DHS job posting for a Technical Cybersecurity Engineer. The essay explores the responsibilities, demands, and standards related to this position. A wide range of technical tasks are included in the duties, with a focus on risk analysis, decision support for DHS leaders, and cooperation with other departments. The crucial nature of the role is highlighted by requirements like citizenship, security clearance, and adherence to professional standards. All things considered, this study emphasizes the importance of the DHS Cybersecurity Engineer - Technical post and its attractiveness to competent applicants.

The Department of Homeland Security is a government entity created around the idea of protecting the people in the United States of America. They have a strong role in matters such as “battling the pandemic, securing the border and administering asylum law, strengthening cybersecurity, preventing violent acts of domestic extremism, and more” (Mission, 2024). This agency has bolstered its efforts since the attack on September 11th. The job listing I have chosen is the job Cybersecurity Engineer - Technical. This job is being hired for by the Department of Homeland Security (DHS). “They are recruiting professionals to support a range of technical skills in Cybersecurity Engineering, Security Analyst, Network Engineer, and Lead Software Developer” (Cybersecurity, 2024). They expect candidates to be able to perform a range of tasks based on your prior experience or education level. This will be a thorough examination of this job listing which will discuss the different needs of the company as well as their expectations towards new hires.

There is a lot of duties to understand when applying for this job in particular. Some of the duties listed imply the idea of working with others. One such duty is “conducting software, hardware, and systems engineering to develop new and refine/enhance existing technical capabilities while ensuring full integration with security objectives, principles, and processes” (Cybersecurity, 2024). This first duty already suggests that the job will require interpersonal skills as well as communication. As a cybersecurity engineer based around the more technical aspect of the job, it would only make sense that someone with this job title may have to operate with the help of different departments in the company. This duty underlines the idea of working with software engineers to conduct software and hardware analysis in order to preserve

system security and capabilities. A second duty is “maintaining security process coordination within the Department’s lifecycle management and governance processes” (Cybersecurity, 2024). This duty suggest working with administration to coordinate the maintenance of security processes. Finally, “Coordinating with systems architects and developers, as needed, to provide oversight in the development of design solutions, system security controls, and countermeasures (including designing and developing new cybersecurity tools/technologies),” this duty explicitly states that someone in this field will have to work with system architects (Cybersecurity, 2024). These seem to be standard duties that would pertain to anyone in the cybersecurity field.

This job also entails “Conducting risk analyses, feasibility studies, and/or trade-off analyses to develop, document, and refine functional requirements and specifications and develop and maintain technical security configuration baselines” (Cybersecurity, 2024). This is something you could find in any job listing for cybersecurity. A lot of the cybersecurity degree at Old Dominion University pertains to risk analysis and such. It is a very crucial part to cybersecurity because it outlines potential risks associated with costs. When it comes to cybersecurity, unless a company has an endless budget, there will always be tradeoffs. Another duty listed that is pretty common in the technical field of cybersecurity would be “assisting DHS leaders with decision-making and actions related to design and implementation of cybersecurity” (Cybersecurity, 2024). A lot of people do not understand the technical terms, so as cybersecurity personnel, it is important to be able to translate into laymans terms. It is also important for a cybersecurity engineer to stay up to date with current technology. The world is evolving

at a rapid pace which only means that the best practices for security will follow behind. This is something the DHS also outlines in the duties for their cybersecurity engineers.

There is a lot when it comes to the requirements of this job. They include, but are not limited to, must be a citizen, must be able to obtain a security clearance, must submit a drug test, and may require a probationary period. These do not surprise me, for this is a government entity. These level of requirements are standard for cybersecurity and government jobs. They also portray a high level of professionalism which speaks to how the work environment may be. When in cybersecurity, information is everything which is why employees are held to these standards. In my opinion, this is a good look on a company when they clearly state the requirements and expectations. Surprisingly the job does not require a certain level of education. Although, the field of cybersecurity does not really require a degree. There are a lot of certifications that someone could get along with experience that could make up for not having a degree.

At the end of the listing, the benefits and salary margins are displayed. I like how they formatted the page putting the benefits last. It is important to understand what you are getting into regardless of the pay. The numbers look good, but expectations must be set early.

Given the analysis of the job listing, this job seems to be crucial for the company as I would expect any cybersecurity job to be. It is very detailed and well throughout. This speakers volumes to the company and their professional outlook. Because the presentation was exceptional, I do believe this job should not be taken lightly. There is a lot to unpack when considering this job, for anyone that would undertake it would be playing a major role in the security of the DHS. I for one would definitely take this job

because it is the exact thing that I have studied for over my time at ODU. I already expected this level of responsibility in a cybersecurity job because of my experience talking with cybersecurity employers and the workforce.

### Works Cited

“Cybersecurity Engineering - Technical.” *USAJOBS*, 7 Mar. 2024,  
[www.usajobs.gov/job/780143700](https://www.usajobs.gov/job/780143700). Accessed 11 Mar. 2024.

“Mission: Homeland Security.” *U.S. Department of Homeland Security*,  
[www.dhs.gov/mission](https://www.dhs.gov/mission). Accessed 11 Mar. 2024.