Writing Assignment One: Job Analysis

Brandon M. Burke

Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Gordon-Phan

January 31, 2025

Abstract

The FBI Special Agent position focused on cybersecurity and IT offers a unique opportunity to apply technical expertise in network security, digital forensics, and related fields to address critical national security threats like cybercrimes, data theft, and ransomware. The role involves a combination of rigorous physical, mental, and technical training at the FBI Academy, followed by hands-on investigative work that can require working irregular hours and being available for assignments worldwide. The job requires a bachelor's degree in a relevant field, at least two years of professional experience, and the ability to obtain a Top Secret SCI clearance. While the ad emphasizes hard skills like cybersecurity knowledge and technical proficiency, it also implies the importance of soft skills such as problem-solving, adaptability, resilience, attention to detail, and time management. The ad's organization highlights the high demands of the job—both in terms of physical readiness and technical expertise—while signaling the need for candidates who are adaptable and able to handle high-pressure situations. Drawing from my coursework in network security, digital forensics, and upcoming internship in cybersecurity, I believe I am well-prepared to meet these technical and personal demands. These experiences have equipped me with the skills necessary to contribute effectively to the FBI's mission of safeguarding national security.

Keywords: Cybersecurity, network security, digital forensics, cybercrimes, FBI

Writing Assignment One: Job Analysis - FBI Special Agent in Cybersecurity

The Federal Bureau of Investigation plays a critical role in safeguarding national security by tackling various criminal activities, including cybercrimes, data theft, and acts of terrorism. One of the most specialized and challenging positions within the FBI is a Special Agent especially in the cybersecurity and technology field. The FBI is seeking candidates with expertise in fields such as network security, digital forensics, and computer science to join its ranks in addressing the growing threat of cybercrimes. This paper will examine the role and responsibilities of an FBI Special Agent with a focus on cybersecurity and IT, analyzing the skills, qualifications, and training required for the position. It will also explore the soft and hard skills that may not be explicitly listed but are essential for success in the role, and reflect on how my own background in relevant coursework and internships has prepared me for these demands.

Overview of the Role and Responsibilities

The FBI Special Agent position, particularly in the realm of cybersecurity and IT, carries a high level of responsibility, requiring candidates to apply technical expertise in investigating cybercrimes, data breaches, and other threats to national security. According to the job description, the core responsibilities of a Special Agent include conducting investigations, executing search warrants, and participating in arrests—all of which may involve responding to urgent threats like ransomware and data theft. Furthermore, agents are expected to work long, irregular hours and be available on-call, ready to handle incidents globally as the need arises. Special Agents must have two years of full-time professional work experience in a related field. In addition, the position demands that applicants complete 18 weeks of specialized training at the FBI Academy in Quantico, Virginia, preparing them for both technical and physical aspects of the job. Additionally, the ad highlights the importance of physical fitness, with candidates needing to pass a medical exam and meet the Bureau's physical requirements, which include maintaining a high level of fitness throughout their career. The role also requires flexibility and the willingness to relocate, as agents are expected to transfer to one of the 56 field offices, which could include remote or international assignments (*Federal Bureau of Investigation Special Agent* 2024). This flexibility, combined with the on-call availability, underscores the demanding nature of the position, where agents must be prepared for any situation at any time.

Qualifications, Experience, Skills, and Training

The ad clearly outlines the technical and professional qualifications required for this position. First, candidates must have a bachelor's degree in a related field such as computer science, network security, or digital forensics. This is a minimum requirement, reflecting the technical nature of the job. Additionally, applicants must have two years of full-time professional experience, either in the field of IT or another related discipline. This experience requirement is a clear indicator that the FBI prioritizes practical knowledge over just academic credentials, seeking candidates who have applied their expertise in real-world scenarios. In addition to having real-world experience and a bachelor's degree, applicants must meet the following qualifications: be a U.S. citizen, be at least 23 years old and have not reached their 37th birthday, be able to obtain a Top Secret SCI Clearance, meet the FBI's employment eligibility requirements, and poses a valid driver's license with at least six months driving experience (*Federal Bureau of Investigation Special Agent* 2024).

On the technical and physical requirements for the job, but not specifically stated, technical expertise in cybersecurity is a critical aspect of the position. Candidates should be skilled in detecting and responding to various types of cybercrimes such as ransomware, data theft, and network intrusions. Moreover, the job should require familiarity with tools, like

Autopsy, and methods used in digital forensics, which involves recovering, analyzing, and preserving electronic evidence in criminal investigations. Incident response is also an essential skill, as agents must quickly and efficiently handle cyberattacks to prevent further damage. Knowledge of firewalls, intrusion detection systems, and data encryption would be essential for the role, as these are commonly used in protecting and securing sensitive information from hackers.

Although the ad is focused primarily on technical qualifications and physical requirements, several important soft skills are implied by the wording of the job description. For instance, the expectation that candidates will work long hours, sometimes with irregular schedules, and be available globally suggests the need for strong time management and stress management skills. The need for agents to make quick decisions during investigations or when responding to cyber threats further points to the importance of critical thinking and decision-making under pressure. Additionally, the ad highlights the need for agents to collaborate with other law enforcement agencies and work on complex investigations, which implies a requirement for teamwork and collaboration. The ability to work well with others, especially in high-stakes environments, is essential. While the ad doesn't explicitly state this, the phrase "work on some of the Bureau's most complex cases" signals that problem-solving and creativity will also be crucial in approaching investigations that often require out-of-the-box thinking (*Federal Bureau of Investigation Special Agent* 2024) In most job listings the importance of these skills to the employer can be determined based on their placement in the advertisement, with the most important being placed first, or early in the listing (Burry, 2022). In my opinion the most important skill is having prior work experience.

In addition to the qualifications, experience, hard skill, and soft skills, a key area of training that would be useful is cybersecurity certifications. Certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and CompTIA Security+ would be extremely beneficial for candidates to have before entering the role. These certifications focus on skills such as ethical hacking, penetration testing, security risk management, and understanding how to defend systems against cyberattacks. Another useful area of training would be in digital forensics. This includes expertise in tools and methods used to gather, analyze, and preserve electronic evidence in criminal investigations. Being proficient in software like EnCase, FTK Imager, or Autopsy can help an agent recover evidence from compromised devices or cloud storage. Programming and scripting knowledge could also enhance an agent's ability to analyze and understand cyberattacks. Knowing coding languages such as Python, JavaScript, and SQL can help when reviewing attack scripts or malware. This can also help them write simple scripts for automating tasks like data collection or analysis. Firearms training would also be important. Executing search warrants can turn into a firefight as seen on news stations countless times from police departments and FBI. Having this training should keep the agent safe and aware of the potential dangers.

Motivators, Reasoning, and Challenges

Considering the context of the job and the company, the FBI's focus on cybersecurity is motivated by the increasing frequency and sophistication of cyber threats to national security. As technology advances, so do the tactics used by cybercriminals, making it crucial for agencies like the FBI to stay ahead of emerging threats. The growing prevalence of ransomware attacks, data breaches, and state-sponsored cyber espionage has created a strong demand for skilled professionals who can protect sensitive information and maintain national security. As cybercrime continues to evolve, the demand for specialized roles like the FBI Special Agent in cybersecurity will only grow.

My interest in the FBI Special Agent position stems from both my technical background and my interest to contribute to national security. I have taken courses in network security, cybersecurity, and digital forensics, which directly connect to the responsibilities of investigating cybercrimes and analyzing digital evidence. The ad mentions tasks such as preventing data theft, ransomware, and securing network security, which are areas that I have experience and am confident in. Additionally, I am confident that my problem-solving and critical thinking skills align with the FBI's need for professionals who can handle complex investigations and respond to cyber threats swiftly and effectively.

The FBI's culture, as reflected in the job description, emphasizes integrity, commitment, and teamwork (*Cybercrime* 2016). The Bureau is known for upholding high standards of conduct, and its focus on national security calls for a strong sense of duty and responsibility. The ad's mention of "adherence to strict standards of conduct" signals a workplace where ethical behavior is of utmost importance (*Federal Bureau of Investigation Special Agent* 2024). However, this does not come without its challenges. Due to the high-stakes investigations involving complex cybersecurity issues, there will be lots of pressure not to compromise an investigation as this can lead to any crime not being solved. Furthermore, the on-call nature of the job and the need to relocate to different field offices could be demanding, as the ad suggests agents should be ready for temporary duty assignments anywhere in the world. Despite this, the high standards and the expectation of continuous professional development at the FBI propose that this role would be rewarding. The ad's clear emphasis on dedication and growth makes the position both challenging and inspiring.

Conclusion

In conclusion, the FBI Special Agent position in cybersecurity is a rewarding role that requires a blend of technical expertise, physical fitness, and strong interpersonal skills. The job, although demanding, involves investigating complex cybercrimes, responding to urgent threats, and working under high-pressure conditions. The qualifications and training required for this role, including expertise in cybersecurity, digital forensics, and network security, are essential for protecting national security in an increasingly digital world. My academic background in network security and digital forensics, along with my desire to contribute to national security, make me a strong fit along with the hard and soft skills needed for this position. Despite the challenges the role presents, the opportunity to work on high-stakes cases and contribute to the safety of the country makes this position both compelling and meaningful.

References

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

Cybercrime. FBI. (2016, May 3). https://www.fbi.gov/investigate/cyber

Federal Bureau of Investigation Special Agent: Cybersecurity/Technology Background. Glassdoor. (2024, December 3). https://www.glassdoor.com/job-listing/special-agent-cybersecurity-technology-background-federal-bureau-of-investigation-JV_IC1130306_KO0,49_KE50,81.htm?jl=1009551306223