Next Five Years

Introduction

In the next five years, I aim to serve as a cybersecurity agent within the government, dedicated to safeguarding our nation from both domestic and international threats. Through my past experiences and ongoing education, I have come to understand that the most perilous battlegrounds of today are not found on physical terrain but within the digital realm of the internet. High-profile incidents, such as the 2017 WannaCry ransomware attack that affected over 200,000 computers across 150 countries, and the massive Equifax breach in the same year that compromised the personal data of approximately 147 million people, highlight the critical vulnerabilities in our digital infrastructure. The unauthorized access and exploitation of personal information, coupled with the burgeoning risks posed by artificial intelligence, are often underestimated.

In response to these alarming developments, I have concentrated my recent efforts on understanding and mitigating the dangers associated with AI. This includes not only developing AI systems but also devising strategies to neutralize and dismantle AI-based threats effectively. For instance, the increasing sophistication of AI-driven phishing attacks, which can now mimic human writing styles to craft deceptive emails, underscores the urgent need for advanced defensive measures. My commitment to this cause is exemplified by my senior project, which focuses on AI-driven email phishing and the generation of malicious AI email chains. Given the rapidly evolving landscape of cyber threats, this area of study is increasingly critical. My goal is

to advance my knowledge and skills in this field to a level where I can offer formidable defenses against these sophisticated and evolving threats.

Once I achieve my professional objectives, I envision a life that balances my career and personal aspirations harmoniously. My dream is to work remotely, nestled in the tranquil expanses of the countryside, potentially in a place like Ocala. This setting would be ideal for building a life with my future wife, whom I have yet to meet, and our two children. I imagine us in a spacious home surrounded by an abundance of land, providing us with privacy and the freedom to explore nature directly from our doorstep.

This land would not only offer a serene backdrop for our family life but also ample space for me to indulge in my passions. I have always been an avid hunter, cherishing the quiet and patient sport teaches, and I see myself continuing this tradition. Additionally, the open fields would be perfect for riding motorcycles, and perhaps by that time, I might switch to a dirt bike to take full advantage of the rugged terrain.

With the increasing possibility of early retirement due to advancements in healthcare and genetic technologies, I aim to secure financial stability early in my career. This strategy would allow me to step back from the workforce at a younger age, thus prioritizing my health and family. The growing prevalence of genetic health concerns has made it even more critical for me to consider a lifestyle that promotes well-being and longevity, ensuring I have quality time to spend with my loved ones and pursue my hobbies.

This vision of remote work, combined with a life deeply connected to nature and family, reflects my desire for a balanced and fulfilling future. It's a life where professional success does not come at the expense of personal happiness and health, but rather enhances it, allowing me to cherish every moment spent under the open sky, with family by my side and freedom at my fingertips.

The Preferred Path

The next few years of my career are strategically planned to encompass both educational advancement and rigorous physical challenges. Initially, my journey will begin in the realm of law enforcement, where securing a position as a law enforcement officer will lay a robust foundation for my future aspirations. This initial role is not just a job; it serves as a pivotal steppingstone towards achieving broader career goals within the government sector.

By starting in law enforcement, I aim to gain invaluable practical experience that will enhance my candidacy for more specialized roles in the future. My ultimate objective within this trajectory is to join the State Police. Recognized as one of the most prestigious law enforcement bodies, the State Police are known for their stringent standards and the elite status of their officers. Achieving a position with the State Police would not only mark a significant milestone in my career but also add a distinguished layer to my professional profile.

This experience would provide me with a substantial government background, enriching my resume and expanding my professional network within federal circles. Moreover, working in this capacity will equip me with a comprehensive understanding of criminal behavior and law enforcement tactics, deepening my knowledge of the legal framework. This criminal and legal insight is crucial, as it will allow me to approach cybersecurity threats with a nuanced perspective that integrates both technical skill and legal acumen.

As I embark on my journey in law enforcement, gaining firsthand experience in the criminal justice field, I am also committed to furthering my education in cybersecurity. I have chosen to pursue a master's degree in Cybersecurity at Grand Canyon University in Arizona, a program renowned for its comprehensive curriculum and expert faculty. This master's program is designed to be intensive yet efficient, requiring only a year and a half to complete.

The structure of the program at Grand Canyon University is tailored to equip students with advanced knowledge and practical skills in cybersecurity. It covers a broad spectrum of relevant topics, including network security, information assurance, ethical hacking, and digital forensics. This will not only enhance my understanding of the digital threats landscape but also refine my ability to develop and implement robust security measures.

By concurrently gaining practical law enforcement experience and advancing my academic credentials in cybersecurity, I am positioning myself uniquely in the field. The combination of real-world law enforcement insights and cutting-edge cybersecurity training will

prepare me exceptionally well for my first specialized role in cybersecurity. This dual focus will enable me to apply a more holistic approach to security challenges, considering both the cyber aspects and the underlying criminal behaviors.

Ultimately, this parallel progression in both practical experience and academic achievement is strategically designed to maximize my readiness and qualifications for a career in cybersecurity, making me a strong candidate for roles that require both tactical knowledge and technical expertise. This comprehensive preparation is essential for effectively tackling the complex cybersecurity challenges faced by government agencies and private organizations alike.

To effectively transition to this next stage in my career, I have invested in professional resume services, recognizing the importance of a well-crafted resume in securing positions in both civilian and federal sectors. This strategic move involved creating two distinct versions of my resume: one tailored for civilian job applications and another specialized for federal employment opportunities. Each version is designed to highlight relevant skills and experiences to meet the specific requirements and expectations of these different sectors.

AUSTIN PAULLEY

Cybersecurity Agent
New Smyrna Beach, FL 32168 | (386) 690-3431 | apaulley@stetson.edu | www.linkedin.com/in/austin-paulley-923b7b27b/

"Leveraging Expertise in AI Development and Cybersecurity to Drive Organizational Initiatives."

Highly organized, results-driven professional with expertise in cybersecurity, leading strategic direction to foster operational excellence and optimize IT efficiency. A skilled collaborator with a proven track record of building and maintaining positive relationships to increase team effectiveness. An expert in AI technologies and operations with a solid comprehension of cyber security needs, aiming to lead strategies that drive workforce efficiency as well as team productivity. Possesses unmatched communication, accuracy, and strong analytical skills, emphasizing a collaborative approach toward leadership. Recognized as an independent leader, committed to professionalism, driven to inspire passion for work, as well as executing innovative strategies to strengthen the organization's capabilities.

CORE EXPERTISE

Cybersecurity | AI Development | Operational Efficiency | Leadership Development | Staff Management | Strategic Planning | Relationship Building | Team Effectiveness | Inventory Management | Analytical Skills | Time Management Skills | Verbal and Written Communication Skills | Quality Assurance | Information Technology | Research | IT Support | Software Systems | Computer Hardware | Technical Support | Information Systems | Internet Connectivity | Troubleshooting

Technical Skills: Java | C++ | Python | Basic Linux | IntelliJ | Docker | Burp | Visual Studio | Kali Linux | AWS servers | HTML and Secure HTML

EDUCATION, CERTIFICATIONS AND PROFESSIONAL DEVELOPMENT

Cybersecurity Major | Stetson University, Deland, FL | August 2022 – Present
GPA of 3.2/4.0 | Full scholarship recipient in Spring 2021 | Part of Stetsons Honors College | Basic Coding, Secure Coding, Network Security, Big Database, Artificial intelligence, and Cybersecurity
Associate of Arts | Daytona State College, Daytona Beach, FL | August 2020 – May 2022
GPA of 3.65/4.0 | Dean's List (Spring and Fall 2021) | Quanta Honors Program designed for high-achieving students.
Certification, Serv Safe Managers | January 2023 – January 2028

PROFESSIONAL EXPERIENCE

Half Wall Port Orange ◆ Port Orange, FL
Kitchen Manager April **2020 – Present**

- Elevate through the ranks from dishwasher to dedicated Kitchen Manager within three years, demonstrating rapid career progression, problem solving, and commitment to operational excellence.
- Implement strategic initiatives and work independently to streamline kitchen operations, optimizing workflow efficiency and fostering a collaborative staff environment.
- Pioneer a targeted and strategic restructuring of staffing, leading to an impressive 25% reduction in inventory costs as well as setting a precedent by achieving the lowest labor costs in the establishment's seven-year history.

VOLUNTEER/LEADERSHIP EXPERIENCE

- Guided emerging leaders within the New Smyrna Beach High School band for a three-year tenure, promoting a supportive and growth-oriented environment.
- Represented the Student Government Association at Daytona State College, actively engaging in how-to guides or decision-making processes and advocating for the student body or problem-solving.
- Devoted more than 350 hours to volunteering throughout the journey, contributing to the enrichment of community programs in Southeast Volusia Babe Ruth and playing an instrumental role in advancing initiatives within the school band.

Jobs Available and Desirable for Someone with My Degree and Experience:

- Cybersecurity Analyst: Monitors networks for security breaches and investigates violations when they occur.
- Information Security Manager: Oversees and coordinates security measures for the protection of computer networks and information.
- Forensic Computer Analyst: Gathers digital evidence from cybercrime scenes and analyzes data to assist in legal proceedings.
- Cyber Intelligence Officer: Works in government agencies to identify threats to national security from cyberspace.
- Network Security Engineer: Designs, implements, and maintains security systems to protect organizations from cyber threats.

Insights from Real-World Job Ads/Openings and Workforce Skills:

Many job advertisements emphasize the need for a mix of educational credentials and practical experience, particularly in systems administration or network management. Roles that appeal to me are those involving varied and complex problem-solving tasks, such as cybersecurity analytics and threat intelligence. However, I am somewhat skeptical about positions that are overly specialized, as they might restrict broad career development. To apply for higher-level positions immediately, I may need additional certifications, such as CISSP or CISM, which I do not currently possess.

In terms of workforce skills, I am equipped with technical proficiency in various cybersecurity software and tools, as well as in network setup and security protocols. My strong analytical thinking enables me to process and interpret large data sets to identify cyber threats, and my problem-solving skills are crucial for diagnosing and mitigating security breaches effectively. Additionally, I am adept at communicating complex technical information in an accessible manner to non-technical stakeholders and can adapt quickly to new technologies and evolving threat landscapes.

Alternative Path

Considering an alternative route to traditional employment and higher education, I am exploring the possibility of joining the intelligence division of the United States Air Force. This path appeals to me not just for the immediate experience and training it offers, but also for the unique opportunity to serve my country while building a specialized skill set in intelligence gathering and analysis.

Choosing this path is motivated by my interest in national security and the sophisticated technological environments that the Air Force is known for. The work in Air Force intelligence would allow me to apply and expand my cybersecurity skills in a highly dynamic and impactful context, engaging directly with matters of national and international importance. This experience would also provide a deeper understanding of global security frameworks, intelligence operations, and the strategic application of cyber technology in defense.

To embark on this path, I must meet the Air Force's rigorous physical and educational standards, which includes completing the Armed Services Vocational Aptitude Battery (ASVAB) to assess my suitability for a role in intelligence. Additionally, I need to undergo a thorough background check to qualify for the necessary security clearances. Preparing for this requires physical training, academic study, and a strong commitment to personal integrity and excellence.

This route is particularly compelling because it offers a blend of immediate job training and experience that is directly applicable to long-term career goals in cybersecurity and national defense, while also fulfilling a desire to contribute meaningfully to the security of my country. The skills, discipline, and networks developed through this experience would be invaluable, whether I choose to continue a career in government or transition to the private sector in the future.

Conclusion

In conclusion, my journey toward a career in cybersecurity and law enforcement is underpinned by a deliberate and well-structured plan that balances education, practical experience, and personal growth. Starting with foundational roles in law enforcement, I aim to build a robust understanding of criminal behavior and legal frameworks, while simultaneously advancing my academic credentials through a master’s degree in Cybersecurity at Grand Canyon

University. This dual approach will prepare me to tackle the evolving challenges of cybersecurity within both civilian and federal spheres.

The exploration of alternative paths, such as serving in the intelligence division of the United States Air Force, underscores my commitment to versatility and readiness to adapt to the dynamic nature of security and technology fields. Each step of this journey is designed not only to enhance my professional qualifications but also to fulfill a deeper commitment to serving and protecting the community and the nation.

Through rigorous preparation, ongoing education, and a strategic approach to career development, I am positioning myself to become a highly competent professional capable of addressing some of the most pressing cybersecurity challenges of our time. Whether through direct law enforcement, federal service, or a combination of both, my career path is geared towards making a significant impact in the field of cybersecurity, contributing to a safer, more secure digital world.

Interview

Name: (Will disclose if asked was asked not to make public)

JOB: DoD Agent

Today I got to sit down with a DoD Agent and talk to them about what are the best features about working for the DoD. He mentioned that one of the best parts is onto of the great benefits there are tons of stuff that you never hear about. Being part of the DoD allows you to travel the world and lets you talk to some of the most interesting people in the world. They said the hours aren't really guaranteed as you work all around the clock and the pay is decent, but the best part is the benefits. They said as far as the education college isn't even important the most important thing is a background in military, law enforcement or some kind of public service. After that they said to really focus on the experience that you have, and the biggest thing is certifications. They said to really focus on security certifications as they will give you a great lead compared to others in the industry. The only stuff I am allowed to put in writing is stuff related to how to get there so for further detail it would have to be privately sent.