

Cover Letter-IDS 493 E-Portfolio Project

Jahmeel Campbell
Old Dominion University
Cybersecurity Major
Fall 2026

Professor Tammy Sommer, MS, Leadership
IDS ePortfolio Project
Old Dominion University

When I look back at everything I have done throughout my cybersecurity degree and especially during IDS 493 I can honestly say this program has changed the way I think and the way I approach my education. I used to think cybersecurity was mostly a technical field such as tools, threats, hacking, vulnerability scanning, patching things like that. But the deeper I got into the program the more I realized it is so much bigger than that. Cybersecurity is legal, ethical, strategic, organizational, psychological and personal. IDS 493 gave me a space to slow down and bring all those pieces together. It forced me to reflect, to organize my work and to understand my academic identity and where I'm headed professionally. Building this ePortfolio showed me that I'm not just getting a degree I'm building a career path grounded in real skills, values and experiences. One assignment that really helped me understand this idea was the Meade chapter discussion on portfolios. Before that reading I thought a portfolio was just a website where you upload your assignments. But while writing the discussion I realized a portfolio is really a story. It's the story of how I've grown, what I've learned and where I'm going. When I wrote about how a portfolio "hits harder" than a résumé because it shows actual proof of your work I realized I was talking about myself. I've done labs, discussions, reports and projects that show my progress not just my participation. That discussion stood out to me because it made me think about how I want employers to view me not as a student who just completed assignments but as someone who has put in real work and can show what he knows. The Meade readings also made me reflect on consistency, discipline and self-assessment. Which are things that matter a lot in cybersecurity more than people realize. The job advertisement analysis assignment was another turning point for me. I chose the Cybersecurity Principal Analyst role at Truist Financial because even though it was a senior-level job it showed me the future direction of the industry. Writing that paper required me to break down the ad line by line, connect it to our course readings and

link it to my ODU courses. That process forced me to look at what employers really want not just technical skills, but also leadership, communication, teamwork and decision-making. When I connected Harper's and Harris & Clayton's readings to the job ad I saw how companies expect a balance of soft and hard skills (Harper, 2012; Harris & Clayton, 2019). The ad listed tools, cloud technologies, zero-trust principles, IAM, SIEM, DevSecOps and more, but it also expected someone who could lead teams, persuade others, manage time and stay calm in pressure situations. Those were the same traits I listed in my values discussion discipline, reliability, calmness and integrity. That connection helped me understand my own strengths more clearly. Another part of that job analysis paper that helped me grow was thinking about company culture and narrative identity. When I looked at Truist's wording "design," "implement," "architect," "ensure," "lead" it made me see how job ads communicate expectations about culture and personality. Atkinson talks about narrative choices and how organizations tell their story through the language they use (Atkinson, 2012). I realized companies want people who can match their story. That made me reflect on my background how balancing school, work at T-Mobile, personal responsibilities and long-term goals taught me consistency and focus. Those qualities match the expectations of a company like Truist. This assignment helped me understand not just the job posting but how I fit into the world of cybersecurity. Another meaningful assignment was the Personal Values Assessment discussion. My top values came out as family, religion, discipline, health, and wisdom. Writing that post helped me realize how much those values show up in everything I do. I wrote about seeing myself as someone who is always trying to better himself spiritually, mentally, and professionally. That is true every class, every shift at work, every assignment I turn in is part of a bigger effort to grow for me. People describe me as reliable, hardworking, respectful, patient, and someone who stays calm even in stressful

situations. Those traits connect directly to cybersecurity roles that require decision-making, clarity and integrity. Writing that post made me understand that my academic identity is not separate from my personal identity. My values show up in my work ethic, my interactions with classmates and professors and the way I handle challenges. My cybersecurity artifacts from other classes also helped me connect what I learned academically to what I'm building professionally. In Cyber Law my discussion on *Van Buren v. United States* pushed me to read a real Supreme Court case and understand how the CFAA is interpreted. That was not an easy assignment because legal language is dense and requires patience. But it helped me understand how laws impact cybersecurity work. I argued that the Supreme Court made the right decision in limiting the CFAA to actual unauthorized access. That assignment showed me how cybersecurity professionals must understand legal boundaries and ethical responsibilities. This connects directly to roles that deal with compliance, auditing and governance roles that appear often in job postings. My risk management discussion helped me realize how risk works across an entire organization. Breaking down assets, threats, vulnerabilities and impacts and applying them to the Equifax breach made me understand how one missed vulnerability can lead to massive consequences. That assignment helped me think strategically not just technically. It showed me how cybersecurity decisions affect finances, trust, public safety, and legal responsibility. When I later looked at the Truist job ad and saw how much they emphasized risk, identity and cloud controls I understood why risk management is at the center of so many cybersecurity roles (Smith, 2019). My CYSE 425W discussion on the responsibilities of national governments versus private firms helped me understand cybersecurity from a national and strategic angle. That assignment was challenging because it required me to think beyond technology and consider politics, ethics, law and policy.

I argued that the government should protect critical infrastructure and defend against nation-state attacks while companies should secure their systems and report incidents. The real solution is collaboration. That discussion helped me understand how cybersecurity fits into the bigger picture of national strategy and public safety. It also helped me see how my classes support each other with law, risk, policy and ethics all connect. Building my portfolio pulled all these lessons together. Going through my old assignments, choosing which ones represented my skills, writing reflections and organizing everything helped me see my growth clearly. I started understanding the idea of “narrative identity” on a deeper level. My portfolio tells a story about discipline, improvement, persistence and learning how to think across different fields. It shows that my academic journey wasn’t random. Every course from IDS 300W to cybersecurity law, risk, policy and technique played a role in shaping me academically and professionally. IDS 300W especially helped me understand integration, analysis and interdisciplinary thinking. Those skills carried over into every cybersecurity class I took. This reflection also made me realize how far I’ve come and how prepared I am becoming for the career I want. The field of cybersecurity requires more than technical skills. It requires communication, adaptability, leadership and integrity. Throughout my degree I’ve built those traits naturally through work, school, assignments and personal growth. Seeing them lined up in my portfolio made me feel confident that I have a strong foundation to start my career. I also want to take time to thank the people who helped me get to this point. First, I want to thank Ms. Lenora, my advisor, for always guiding me, helping me stay on track, and supporting me throughout my time in this program. Her advice and patience made a big difference especially during the times when I felt overwhelmed or unsure about my next steps. She always made sure I had what I needed and understood what paths were best for me academically and I appreciate her more than words can

describe. I also want to thank my professors across the Cybersecurity program, especially the ones who pushed me, challenged me, and helped me grow even when I didn't realize it at the time. Whether it was breaking down a Supreme Court case, learning how to manage organizational risk, writing about national cybersecurity responsibilities, practicing technical skills or learning how to think across disciplines. Every professor added something to my academic journey. Their guidance, feedback and teaching helped prepare me for the real cybersecurity world and I'm forever grateful for every moment. This degree and this course helped me become a better student/man and a better future cybersecurity professional. IDS 493 helped me see how everything connects my values, my skills, my coursework, and my future career. It showed me that interdisciplinary thinking is not just something you learn in school, it's something you need in cybersecurity because the field crosses so many areas. After completing this reflection and building my portfolio, I feel more focused, more confident and more prepared for whatever comes next.

References

Atkinson, R. (2012). *The life story interview*. Sage Publications.

Harper, D. (2012). *Visual sociology*. Routledge.

Harris, R., & Clayton, B. (2019). Generic skills and organizational expectations: Employer perspectives in modern workplaces. *International Journal of Training Research*, 17(3), 208–223.

Henry, S. (2012). Ethics and social responsibility in information technology. *Journal of Information Ethics*, 21(1), 45–56.

Nguyen, T. (2019). The rising importance of soft skills in cybersecurity careers. *Cybersecurity Journal*, 4(2), 55–64.

Smith, J. (2019). Workforce trends in cybersecurity: Skills, hiring, and future demand. *CompTIA Cyberstates Report*.

Truist Financial Corporation. (2024). *Cybersecurity Principal Analyst job posting*.

Meade, K. (n.d.). *Looking at your strengths and values*.