Reflective Essay: The Skills I've Acquired

CJ McDonald

Old Dominion University

IDS 493: Electronic Portfolio Project

Professor Carin Andrews

November 15, 2025

Introduction

As I come to the end of my Cybersecurity degree at Old Dominion University, I have been able to look back and really see how my classes, projects, and writing assignments have shaped the skills I am taking with me into my career. When I first started, I mostly thought about cybersecurity as technical work—networks, systems, and tools. Over time, I realized that strong cybersecurity also depends on understanding policy, thinking critically about complex problems, and explaining ideas clearly to different audiences.

The three main skills that stand out for me are Cyber Risk and Compliance, Critical Thinking and Problem Solving, and Research and Cyber Policy Analysis. These skills did not come from just one class. They developed through a mix of cybersecurity courses, writing-intensive classes, and interdisciplinary projects like Innovate Cyber and the U-OVN pitch competition. The nine artifacts in my ePortfolio show how these skills grew across different disciplines and how they line up with what I see in job ads for roles like cyber risk analyst, GRC analyst, and cybersecurity policy analyst.

Skill 1: Cyber Risk and Compliance

My first key skill is cyber risk and compliance. I built this mainly in CYSE 430: Intro to Cyber Risk Management, where I had to connect technical security concepts with legal requirements and business priorities. My first artifact for this skill is my CYSE 430 final exam essay, Final Exam: Risk Mitigation Strategies. In that exam, I had to pull together everything from the course—risk assessments, business impact analysis, business continuity, disaster recovery, and incident response—and explain how an organization could use those pieces to stay resilient. Writing it made me think through how leaders decide which systems are mission-critical, how

they set recovery time objectives, and how they justify investments in backup and recovery. Instead of just listing terms, I had to show how a risk management program would actually work in a real organization, which is what many job ads describe when they ask for understanding of risk frameworks and the ability to communicate risk to stakeholders.

The second artifact is my Chapter 10 Reflection: Planning Risk Mitigation Throughout an Organization. In this reflection, I wrote about how risk mitigation is not just a one-time project but an ongoing process across all seven IT infrastructure domains. I talked about identifying assets, threats, and vulnerabilities, then selecting controls using frameworks like NIST SP 800-53 and thinking through cost–benefit analysis. While I was writing, I found myself bringing in ideas from business and even some basic economics, because it is not realistic to apply every control everywhere. That connection across disciplines helped me see risk management as a balance between security, usability, cost, and compliance.

The third artifact for this skill is my Chapter 3 Reflection: Understanding and Maintaining Compliance. This reflection focused more on laws and standards, such as FISMA, HIPAA, PCI DSS, and the NIST Cybersecurity Framework. I wrote about how these rules shape what organizations must do and how failing to follow them can lead to real consequences, including fines and loss of trust. I also reflected on breach case studies and how some companies were technically compliant but still got breached. That pushed me to see compliance as a baseline, not the final goal. Combining what I learned in this course with my broader understanding of ethics and policy helped me build a more complete picture of what cyber risk and compliance work looks like in the real world.

Skill 2: Critical Thinking and Problem Solving

My second major skill is critical thinking and problem-solving. I developed this mostly through hands-on, design-based projects where there was no single “right” answer. The first artifact here is the Innovate Cyber 2024 – EncryptX website prototype. In that project, my team had to identify a real user problem related to secure communication and then design a solution that people would actually use. Instead of just building something that sounded cool, we had to ask questions about what users needed, what constraints we had, and how to balance security and usability. I remember going back and forth on which features were really essential and which ones were just nice to have. That process taught me how to break a big problem into smaller pieces and make tradeoffs instead of trying to do everything at once.

The second artifact is the Innovate Cyber 2025 – Internet Explorers website. This time, I approached the project differently because of what I had already learned. Instead of starting from zero, my team looked at what had gone wrong or felt clunky in the 2024 project and tried to improve on it. We mapped out where users might get confused, ranked changes by impact and effort, and then focused on what would make the biggest difference. This kind of iteration, where we used evidence from our first attempt to guide our next one, really strengthened my problem-solving skills. It felt similar to how cybersecurity teams improve processes over time—responding to incidents, learning from them, and adjusting controls and workflows.

The third artifact for this skill is the U-OVN K–12 AI Assistant Pitch Canvas. This project was different from my usual cybersecurity work because it was centered on education and student experience. My team had to design an idea for an AI assistant that could support K–12 learning,

and we needed to think about things like classroom management, accessibility, equity, and privacy. The pitch canvas format required us to clearly lay out the problem, key stakeholders, assumptions, tests, and success criteria. I had to think critically about how our solution might impact teachers and students, not just whether the technology was possible. This experience showed me that my problem-solving process can carry over into other fields and that interdisciplinary thinking—combining technology, education, and ethics—is essential when designing solutions that affect real people.

Skill 3: Research and Cyber Policy Analysis

My third skill is research and cyber policy analysis, which grew through my writing-intensive cybersecurity policy course, CYSE 425W. The first artifact in this category is CISA: A Policy Analysis Review. In this paper, I focused on the Cybersecurity Information Sharing Act (CISA), explaining its main goals and requirements in plain language. I researched the major incidents and political pressures that led to the law, then connected CISA to the broader U.S. national cybersecurity strategy. Writing this paper helped me practice finding credible sources, organizing them around a clear argument, and explaining how law and policy interact with technical security challenges.

The second artifact is Ethical Implications of CISA. This assignment pushed me to look at CISA through an ethical lens. Instead of just asking whether it worked, I had to ask whether it was fair, who it protected, and who might be put at risk. I discussed tradeoffs between national security, privacy, and civil liberties. To do that, I drew on concepts from ethics and political science, not just cybersecurity. This made me think more critically about how policy decisions can have very different impacts on different groups of people.

The third artifact is Social Implications of CISA. In this paper, I explored how CISA affects society as a whole, including public trust, power dynamics between large and small organizations, and cultural attitudes toward surveillance and data sharing. I connected the policy to real-world examples and discussed how it might shape behavior over time. These three papers together show that I can read complex policy language, research context, and impacts, and communicate my analysis in a clear, structured way. When I look at job ads for analyst and GRC roles, many of them mention interpreting policies, writing reports, and communicating implications to management. My policy writing experience has helped me build exactly those skills.

Conclusion

Looking across all three skills and nine artifacts, I can see how my program has shaped me into an interdisciplinary cybersecurity professional. Courses like CYSE 430 built my foundation in risk and compliance by mixing technical content with legal and business perspectives. The Innovate Cyber and U-OVN projects helped me practice critical thinking and problem-solving in messy, real-world situations where I had to work with teammates and think about users. The CYSE 425W papers trained me to research, analyze, and write about policy and ethics in a detailed and organized way.

Courses like IDS 300W also played an important role by introducing me to interdisciplinary methods and making me think about how different disciplines talk to each other. I learned how to reflect on my own learning, how to connect theories from one class to projects in another, and how to explain my work to people outside of cybersecurity. Overall, this program has shown me

that being an effective cybersecurity professional is not just about knowing tools and technologies. It is about being able to think across disciplines, understand the bigger picture, and communicate clearly. Those are the skills I will carry forward as I move into cyber risk, compliance, and policy-focused roles.

References

Barrett, M. P. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. *NIST Cybersecurity Framework*, *1.1*(1.1). http://dx.doi.org/10.1002/https://dx.doi.org/10.6028/NIST.CSWP.04162018

CISA. (2015). *TITLE I-CYBERSECURITY INFORMATION SHARING*. https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf

Congress.gov. (2013). *S.2521 - 113th Congress (2013-2014): Federal Information Security Modernization Act of 2014*. Congress.gov. https://www.congress.gov/bill/113th-congress/senate-bill/2521

Federal Information Security Modernization Act | CISA. (2025). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/federal-information-security-modernization-act?

H.R.3103 - 104th Congress (1995-1996): Health Insurance Portability and Accountability Act of 1996. (2019). Congress.gov. https://www.congress.gov/bill/104th-congress/house-bill/3103

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996. (n.d.). Retrieved November 16, 2025, from https://www.cms.gov/files/document/hipaalawdetailpdf?

McDonald, C. (2024a). *CISA: A Policy Analysis Review*.

McDonald, C. (2024b). *Ethical Implications of CISA*.

McDonald, C. (2024c). *Simple Statement*.

McDonald, C. (2024d). *Social Implications of CISA*.

McDonald, C. (2025a). *Chapter 3 Reflection: Understanding and Maintaining Compliance*.

McDonald, C. (2025b). *Chapter 10 Reflection: Planning Risk Mitigation Throughout an Organization*.

McDonald, C. (2025c). *Final Exam: Risk Mitigation Strategies*.

McDonald, C., & Knickelberry, K. (2021). *Home | Encryptx*. Encryptx. https://knick004.wixsite.com/encryptx

McDonald, C., & Knickelberry, K. (2023). *Home | WeDu*. Internet Explorers. https://knick004.wixsite.com/internet-explorers

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity*, *1.1*(1). https://doi.org/10.6028/nist.cswp.04162018

NIST. (2020, September 23). *Security and Privacy Controls for Information Systems and Organizations*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST. (2025). *Cybersecurity Framework*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

PCI Security Standards Council. (2018). *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. Pcisecuritystandards.org. https://www.pcisecuritystandards.org/document_library