**Cybersecurity Graduate Capstone**

**Topic Approval Form**

*The guidelines for the capstone course require a student to demonstrate the application of academic and professional abilities developed as a graduate student. The capstone challenges students to integrate skills and knowledge from several program domains into one project. As a result, it is highly recommended your topic resolve a current or perceived business problem. As stated, you want to exemplify what you have learned in your cybersecurity graduate program to showcase your skills. Remember, your research topic exemplifies scholarship and research at the highest level and is significant and helpful to potential employers in identifying your abilities. Your research will always be something you can look back on with pride. Finally, it is recommended for students to use publicly available data sets for transparency and external validity.*

*The purpose of this document is to help you clearly state the research question you will be exploring in your capstone project, your project’s scope, and your timeline in order to ensure these align with your degree emphasis. Without clearly defining each of these areas, you will not have a complete and realistic overview of your project, and it cannot be accurately assessed whether your project will be acceptable for the purposes of these courses. Of course, if this is a project you have already completed at work or elsewhere, this form should be easy to complete. Many students use a project they have already completed in the past several years. In that case, you will write the proposal as if the project has not been done yet, and when you report on your project, you will use your complete after-implementation report. If you have not yet done your project, this document can help ensure the scope is within the acceptable range for this capstone. An instructor will approve this form before submitting this task for evaluation. The task will not be evaluated without an instructor’s signature. The instructor may ask for additional information before approving the form.*

*Before submitting this form for approval, please remove page 1 from the form.*

***Please only submit a Topic Approval Form that has been signed by an Instructor for evaluation.***

**Cybersecurity Graduate Capstone**

**Topic Approval Form**

The purpose of this document is to help you clearly state the research question for this capstone project, as well as your project’s scope and timeline, to ensure these align with your degree emphasis. While you may not have a complete and realistic overview of your project at this time, the acceptability of your project for the purposes of this course cannot be accurately assessed without clearly defining each of these areas. Many students use a project they have already completed within the past two years. If you choose a finished project, you will write the proposal as if the project is not yet complete. Then, when you report on your project, use your complete after-implementation report.

If you have not yet started your project, this document can help ensure the scope is in the acceptable range for this capstone. An instructor must approve this form before you submit your capstone for evaluation. The task will not be evaluated without an instructor’s signature. The instructor may ask for additional information before approving the form.

**Student Name:** Damian J. Yates

**Student ID:** 000478522

**Capstone Project Name:** Improving Cybersecurity Posture for Small Businesses and Nonprofits

**Project Topic:** Developing a NIST-aligned cybersecurity framework and deployment plan tailored for small, rural, and nonprofit organizations with limited resources.

**Summary of the Problem:** Many small businesses and nonprofit organizations operate with outdated infrastructure and limited cybersecurity awareness. These limitations increase the risk of data breaches and cyberattacks, which could endanger community services and sensitive information.

**Outline of a Technology-Supported Security Solution:** This project will deliver a security framework built upon NIST CSF and CIS Controls v8, deploy basic tools (MFA, secure email, antivirus), and provide training materials. Open-source tools will be used to ensure accessibility and affordability.

**Context:** *Explain why the situation or question would benefit from your security solution.*These underserved organizations serve vulnerable populations but lack the IT capacity to secure operations. A scalable, repeatable framework would provide critical protection and elevate trust with partners, donors, and clients.

**Stakeholders:** *Identify the project stakeholders.*  
- Executive Director   
- Staff and Volunteers   
- Donors and Grant Providers   
- Yates Enterprise Solutions (project sponsor)

**Project Plan:** *Describe the project plan, scope, goals, and objectives.*  
**- Scope**: Apply to one nonprofit organization; create documentation usable by others.   
- **Goals**: Improve security posture; provide tools and processes.   
- **Objectives**: Risk assessment, solution deployment, training, and documentation.

**Methodology:** *Outline the project approach.*   
- Conduct interviews and baseline assessments.   
- Align tools and processes to NIST/CIS standards.   
- Deploy security tools and gather post-deployment metrics.   
- Collect feedback and revise documentation.

**Implementation Plan:** *Identify the project phases*.   
- Research and planning (Week 1–2)   
- Risk and needs assessment (Week 3)   
- Design and document the solution (Week 4–5)   
- Deploy and test (Week 6)   
- Training and knowledge transfer (Week 7)   
- Final reporting (Week 8)

**Project Outcomes:** *List the key anticipated project outcomes and deliverables in 500 words or less*.   
- A documented security framework for low-budget organizations.   
- A repeatable playbook for other nonprofits.   
- Measurable improvement in security posture (e.g., phishing test results, endpoint protection score).   
- Increased staff awareness based on training assessments.

**Projected Project End Date:** 7/25/2025

**Sources:** *Include a list for all references and citations that support the summaries above and are used in-text and as outside sources.*   
- NIST Cybersecurity Framework   
- CIS Controls v8   
- OWASP Foundation   
- SANS Institute

**INFORM YOUR INSTRUCTOR OF THE FOLLOWING:**

Potential use of human subjects (Y/N): N

Potential use of proprietary company information (Y/N): N

**STUDENT SIGNATURE:**

**­­­­­­­­­­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**By submitting this form, you acknowledge** **all information provided is accurate, and any changes to the topic, proposal, or goals must be discussed with your assigned instructor prior to continuing.**

**INSTRUCTOR NAME:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**INSTRUCTOR SIGNATURE:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**INSTRUCTOR APPROVAL DATE:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**