

From: [Smith, Randy](#)
To: [Armstrong, Julia N.](#); [Mick, Robert](#)
Cc: [Leite, Fabio](#); [Reed, Katie](#); [Smith, Randy](#); [Miriti, Maria](#); [Stromberger, Mary](#); [Duffy, Lisa](#); [Quinzon-Bonello, Rosario](#); [Tomasko, David](#); [Howard, Ayanna](#); [Gardner, Jared](#); [Clark, Caroline](#); [Watson, Sara](#); [Greenbaum, Rob](#); [Griffiths, Rob](#)
Subject: Proposal to establish a Master of Cybersecurity and Digital Trust
Date: Friday, June 21, 2024 12:48:10 PM
Attachments: [image001.png](#)

Bob and Julia:

The proposal from the College of Engineering to establish a Master of Cybersecurity and Digital Trust degree program was approved by the Council on Academic Affair at its meeting on June 14, 2024. Thank you for attending the meeting to respond to questions/comments.

The proposal will now be sent to the University Senate with a request to be included for action at the Senate meeting on **September 21, 2024**. The Chair of the Council will present the proposal, but we will need you or a designee to attend to respond to detailed questions. Prior to that it will need discussion at the Faculty Council on **September 7, 2024**, and the Senate Steering Committee on **September 14, 2024**. I will provide you with details as I receive them.

If approved by the Senate, the proposal will be sent to the Board of Trustees for action at its meeting on **November 20, 2024**.

The Graduate School will now work with you on the approval process with the Ohio Department of Higher Education.

The Office of the University Registrar will contact you if there are any implementation issues.

Please keep a copy of this message for your file on the proposal and I will do the same for the file in the Office of Academic Affairs.

If you have any questions please contact the Chair of the Council, Professor Fábio Leite (.11), or me.

I wish you success with this important program development.

Apologies for the delay in sending this message. I have been out of the country all week.

Randy



W. Randy Smith, Ph.D.

Vice Provost for Academic Programs

Office of Academic Affairs

University Square South, 15 E. 15th Avenue, Columbus, OH 43201
614-292-5881 Office

smith.70@osu.edu

Assisted by:

Katie Reed

Executive Assistant

(614) 292-5672

reed.901@osu.edu

TO: Randy Smith, Vice Provost for Academic Programs

FROM: Graduate School Curriculum Services

DATE: **3/01/2024**

RE: Proposal to **Establish a Master in Cybersecurity and Digital Trust** in **Engineering**

The **Department of Electrical and Computer Engineering** in the **College of Engineering**, in collaboration with the Department of Industrial and Systems Engineering and the Institute for Cybersecurity and Digital Trust is proposing a **Master in Cybersecurity and Digital Trust**.

The proposal was received by the Graduate School on **1/08/2024**. The combined GS/CAA subcommittee first reviewed the proposal on **2/14/2024** and requested revisions. Revisions were received on **2/24/2024**. GS/CAA conducted a second review of the proposal on **2/28/2024**. The proposal is supported for elevation to CAA for review.



Memo


To: Dean Maria Miriti, Graduate School
From: Rosie Quinzon-Bonello, Assistant Dean for Curriculum and Assessment
Date: January 8, 2024
Re: Proposal for On-line Degree Program - **Master of Cybersecurity and Digital Trust (MCDT)**

On Monday, December 4, 2023, the College of Engineering Committee for Academic Affairs unanimously approved the proposal for the on-line degree program, Master of Cybersecurity and Digital Trust (MCDT), with the following request:

- A supplementary statement be written in collaboration with the Department of Integrated Systems Engineering (ISE) articulating the importance of including human factors in a program to educate students about cybersecurity and digital trust.

This information was requested, received, and summarized (due to character restrictions) on page eight under the section *Content Growth*. The full statement from ISE can be found in the Addendum on page fourteen.

Yours sincerely,


Rosie Quinzon-Bonello

February 23, 2024

GS/CAA Committee,

I appreciate your consideration for the approval of a Masters in Cybersecurity and Digital Trust. Your feedback was well received, and we have adjusted accordingly. Page numbers were added to the document in the footer for clarity. Those are referenced in these notes:

1. On pg. 7 of the proposal, at top of the page, the word “educational” was added to refer to the breadth of *educational* diversity.
2. On pg. 6 of the proposal, in the second full paragraph, there is a slight rewrite to describe the regional program.
3. As a point of clarification, the proposal addendum (pg. 15) was requested by the College of Engineering’s CAA. We are communicating our plans for growing the elective course options for the MCDT. This is not to be confused with the proposal curriculum as written.
4. The ‘course blocks’ on pg. 8 have been reorganized to indicate core courses, topical themes, and then the elective list. In addition, language throughout the proposal has been slightly amended to use the word “topics” instead of “tracks”. While it is one master’s degree, the wording helps to set apart the contributions from two departments.

Sincerely,

Julia Armstrong
Managing Director, ICDT
armstrong.798@osu.edu
614-688-1909

CCGS NEW PROGRAM PROPOSAL INSTRUCTIONS

The CCGS requirements for proposing a new degree program have been aligned to mirror requirements in the *Substantive Change Application* from the Higher Learning Commission. This will reduce the work of those who propose programs, when there is a need for institutional submission of approved programs to HLC.

Work with your Graduate School to make sure you have all the most current forms needed to complete the proposal. For example, if the program will go directly online, the *Online/Blended Delivery Form* should also be submitted (this can be obtained from your Graduate School offices).

The following template should be followed when creating a proposal for a new degree program. All indicated sections must be included in the Proposal. In the template, *text in italics* are instructions or examples that should be replaced with your proposal text. A maximal length is provided for some sections, to provide guidance about the level of detail that is expected.

Once complete, convert the proposal document to a PDF.

The proposal document should be submitted with a separate Appendix in a second PDF file, containing:

1. **A Table of Contents** for the Appendix
2. **Faculty Matrix.** *A template for this Table is at the end of this document. A faculty member must be identified for each course that is a required component of the curriculum, and the goal of this matrix is to summarize faculty credentials and course involvement. Note that this matrix should also include any projected faculty hires that are needed to support the program.*
3. **2-page Vitae for each faculty member involved in the program.** *NOTE: each vita is limited to 2-pages and should provide information that establishes faculty credentials and expertise to support their role(s) (e.g. teaching, research mentor) in the program.*
4. **Course Descriptions**, each maximally a paragraph in length. *Provide course numbers for existing courses, and indicate those courses which are not yet implemented/approved. Do not include course syllabi.*
5. **Fiscal Impact Statement.** *Include an Ohio Department of Higher Education Fiscal Impact Statement (FIS) which will be used to demonstrate institutional plans for the judicious use of resources in terms of physical plant, personnel, student support, and appropriate institutional commitment of resources to the new program. The most current FIS form may be obtained from your Graduate School offices.*
6. **Market Analysis and/or Needs Survey.** *Market analysis via the Bureau of Labor Statistics projections (<https://www.bls.gov/emp/data.htm>) or software such as Burning Glass/Labor Insights is strongly suggested. Supply summarized data from any survey (detailed data and testimonials not needed).*
7. **Letters of Support.** *Include as appropriate to the institution and program being proposed. (e.g., Provost, Dean, Department Chair(s), internal/external collaborators, outside experts, etc.)*
8. **Consultant reports, if applicable.**
9. **CCGS Online/Blended delivery form, if applicable.** *The most current form may be obtained from your Graduate School offices.*

**Proposal to the Chancellor's Council on Graduate Studies
for a new degree program:**

Master of Cybersecurity and Digital Trust (MCDT)

Mode of Delivery: *fully online*

Submitted by
The Ohio State University College of Engineering

Institute for Cybersecurity and Digital Trust
Department of Electrical and Computer Engineering
Department of Computer Science and Engineering

Revised February 22, 2024

BASIC CHARACTERISTICS OF THE EDUCATIONAL PROGRAM

1. Brief description of the disciplinary purpose and significance of proposed degree.*(max 300 words)*

We are seeking approval for a graduate program to award students a Professional Master's degree in Cybersecurity and Digital Trust. The program's primary goal is to supply highly skilled individuals to the cybersecurity workforce in Ohio and across the nation. Graduates will be trained in well-established and emerging areas of cybersecurity and meet the rapidly growing demand for well-trained cybersecurity professionals. A primary focus of the proposed degree program is the training of professionals in the workforce who seek to become experts in cybersecurity and digital trust. This program is designed as a Professional Master's degree, as opposed to a research-oriented one, in that it focuses on imparting cybersecurity knowledge and skill sets relevant to existing and emerging positions in the workforce. The training is heavily tilted towards application of these skills and knowledge to solving problems encountered at the workplace daily. With the provided training, the graduates will be ready for employment in various industrial and government institutions, especially in Ohio, while benefiting from The Ohio State University's established environment of diversity, ethics, responsibility, and professionalism.

The program will be offered fully online: This will address the existing educational constraints of the ongoing COVID-19 pandemic and lay the foundation of growth into national and global markets without being geographically constrained. The experimental nature of the subject is carefully adapted to the online learning modalities and supplemented with experimental platforms that are globally available. The graduates of the program will be trained by experts of The Ohio State University as well as by our industry partners, who have well-established track record of cybersecurity training excellence. Equipped with both theoretical as well as practical skillsets, the graduates will have opportunities to transition to high-skill cybersecurity and digital trust positions and become leaders in their organizations.

2. **Definition of the focus of the program.** *(max 300 words) This is only intended to be an overview. Make sure to explicitly identify if plans include defined lines of curricular focus within the degree program (tracks or concentrations) and whether they will be noted on the transcript.*

The focus of the program will be to educate and train students and working professionals in the area of cybersecurity and digital trust, within two highly-focused tracks (topical areas). The required curriculum will be a combination of didactic and experience-based coursework components. The curricular tracks are designed consistent with the program's mission of educating and training students with skills necessary in the workforce. The tracks of the program reflect the workplace needs of cybersecurity expertise and allow the participants to be trained in sub-areas that match their interests and backgrounds. The degree program will consist of two tracks, focusing on design & implementation and offense & defense.

3. **Rationale for degree name.** *(max 100 words)*

Professional Master of Cybersecurity and Digital Trust (MCDT) reflects the program's objective of educating students with fundamental and cutting-edge knowledge in cybersecurity and digital trust areas and preparing them for direct employment in the workforce. It is essential that all engineering professionals recognize that cyberspace is a sociotechnical system, or rather a system of systems, both technical and social. These should be equally valued and attended to in the effort to create 'trustworthy' digital systems.

4. **Duration of the program.**

a. **Total credit hours.**

A minimum of 30 semester credit hours will be required to earn the Professional Master of Cybersecurity and Digital Trust degree. This minimum number is on-par with other online master's degrees on cybersecurity topics. Our program is structured clearly and builds in-depth knowledge in two selected tracks/topics with both theoretical and application-oriented courses as well as a mandatory project-oriented course. The application of cybersecurity principles to problems encountered in various workplace scenarios is central to the design of all courses. The project-oriented course is designed as a degree culmination point, where students collaborate to apply their gained knowledge and skills to solve larger scale cybersecurity problems in a collaborative group setting.

The MCDT degree requirement is the completion of the requirements of two topics, each of which requires 6 credit hours of coursework. In addition to the topical completion requirements, students will be required to take a 3-credit hour introduction to cybersecurity course, a 3-credit hour cybersecurity ethics course and a 3-credit hour project-oriented course.

b. **Normal or typical length of time for students to complete the program.**

The curriculum is designed to be completed in two semesters, typically spanning Autumn and Spring semesters of the same academic year. However, the curriculum has been designed to accommodate students taking courses at a slower pace (e.g., 6 credit-hours per semester for 5 semesters), specifically catering to the needs of students who are already in the workforce.

5. **Admission timing.**

The proposed date for implementation of the program is August 2024. It is expected to admit new cohorts every autumn and spring term. It is anticipated that the program will admit one cohort 50 students in its initial offering and reach an enrollment of 150 students in by the end of three years. At

steady state, the enrollment is expected to be 300 students per year.

6. Primary target audience for the program and admission requirements. (max 300 words)

There are two primary target audiences for this program: 1- Students who recently received their BS degrees, 2- Professionals employed in the workforce. Since the program is offered fully online, students can complete the course while being employed full or part time.

Students accepted to the program would be expected to hold a Bachelor's degree in a field related to computer science, cybersecurity, electrical or computer engineering, or information technology. Students with Bachelor's degrees in non-traditional backgrounds and degrees will be accommodated if they provide evidence of in-workforce experience and/or training in relevant topics.

Recruitment and processing of admission's applications will be managed through the Professional and Distance Education Programs office and adhere to an application process with the following qualifications:

- A personal statement of why the applicant is applying to the program
- An official transcript with proof of completed Bachelor's Degree (or higher) in any of the areas related to the program tracks, or a Bachelor's degree supplemented with proof of completion of professional training and experience in related areas.
- Three letters of recommendation.
- All international applicants whose native language is not English will be required to take the Test of English as a Foreign Language (TOEFL) and have an official score report sent directly to the Associate Dean for Graduate Studies from Educational Testing Service. The recommended minimum TOEFL scores are 560 (written) or 220 (electronic) or 89 (internet based).

Evaluation of applicants for admission to the program will be managed by the MCDT-GSC who will adhere to the principles of *individualized holistic review*. Therefore, GPA and test scores will be considered as contributors in the admissions process, but not exclusive criteria for admission into the program.

7. Special efforts to enroll and retain underrepresented groups. (max 500 words) *Offer plan to ensure recruitment, retention and graduation of groups underrepresented within the discipline. Provide as background (1) Institution and department profiles of total enrollment and graduate student enrollment of underrepresented groups within the discipline, and compare to (2) nationally reported values from NCES, Council of Graduate Schools, or other authoritative sources. Supply data by demographic group where available. Your Office of Institutional Research, or the Graduate School, can assist in gathering this data.*

We plan to work with our collaborating departments and colleges to facilitate recruitment and retention of minority students. Special efforts will be made to recruit and retain underrepresented groups in this program. We will work closely with The Community, Access, Retention and Empowerment Office (CARE) in the College of Engineering to recruit members of underrepresented groups into this program and retain them in the program to matriculation. We will coordinate our efforts in recruitment, admission, and retention of underrepresented groups with the CoE's ongoing and emerging initiatives. A key part of our efforts will include collaborations with employers in Central Ohio to reduce the financial burden on URM students through scholarships and employee contributions.

The College of Engineering had 350 new students (99 female) enroll in a master's program in 2022. Of those, 69 (21 female) were in Computer Science and Engineering, and 75 (14 female) in Electrical and Computer Engineering. For the College of Engineering, 138 of 350 identified as White. Comparatively, only 12 out of 69 in CSE and 16 out of 75 in ECE identified as White. In both programs, international students make up over 60% of the masters' enrollment. Per the Society of Women Engineers, the 2019-2010 master's degrees nationwide were awarded to 30.3% women. This is comparable to the 21 of 69 in the CSE master's program recently. The NSF reported that as of 2021, Science & Engineering (S&E) graduate students at the master's level are 57.6% White and 13.1% Asian.

INSTITUTIONAL PLANNING FOR THE PROGRAM

1. What are the physical facilities, equipment and staff needed to support the program?

The Professional Master of Cybersecurity and Digital Trust (MCDT) program will be housed in The Ohio State University College of Engineering. The program is being proposed by the Department of Electrical and Computer Engineering and the Department of Computer Science and Engineering. The program will be executed in partnership with the Institute for Cybersecurity and Digital Trust and Professional and Distance Education Programs (PDEP) in the College of Engineering.

The MCDT degree will be administered by the College of Engineering through the Professional and Distance Education Programs Office. The MCDT Graduate Studies Committee (GSC) will be established within the College to coordinate the oversight of the program.

a. Graduate Studies Committee (GSC)

An MCDT Faculty Director will act as the chair of the MCDT-GSC. The MCDT-GSC will be responsible for all curricular oversight, assessment of the degree, and the evaluation of applicants for admission to the degree. The MCDT-GSC will consist of these voting members, the MCDT Faculty Director, one representative from the Department of Electrical and Computer Engineering, one representative from the Department of Computer Science and Engineering, one representative from the Institute for Cybersecurity and Digital Trust. The MCDT-GSC will include the College of Engineering Director of Professional and Distance Education Programs, as a non-voting member.

b. Office of Technology and Digital Trust (OTDI)

The proposed program will be developed in partnership with the Office of Technology and Digital Trust.

c. MCDT Operations

The Director of Professional and Distance Education Programs in the College of Engineering and their staff will be responsible for the overall administration and day-to-day operations of the degree.

Significant support from the faculty and staff in the Institute for Cybersecurity and Digital Trust will also be involved to support admissions, advising and program development through monitoring and continuous improvement of courses and growth of the program offerings.

- 2. What is the evidence that a market for the new program(s) exists? How has estimated program demand been factored into realistic enrollment projections? How has this evidence been used in planning and budgeting processes to develop a quality program that can be sustained?** *(max 500 words) Using information added to the Appendix, provide evidence of need for the new degree program, including the opportunities for employment of graduates. Examples of potential metrics supporting program need include: Student interest and demand (Potential enrollment; Ability to sustain the critical mass of students. Surveys of potential student interest can be helpful); Institutional need (Plan for overall development of graduate programs at the proposing institutions); and, Societal*

demand (Intellectual development; Advancement of the discipline; Employment opportunities to meet regional, national and/or international needs).

Per the market survey report conducted in October 2020, cybersecurity professionals are employed in almost all medium-to-large scale corporations, federal and local governmental entities, and the military. Employers demonstrate robust demand for master's-level cyber security studies professionals. From September 2017 to August 2020, relevant regional and national employer demand increased faster than demand for master's-level professionals over all (i.e., 2.05 percent per month compared to 0.33, and 2.10 percent per month compared to 0.44 percent, respectively). Additionally, four of five regional and all five national top occupations relevant to master's-level cyber security studies professionals are projected to grow faster than all occupations.

The Ohio State University's plan to launch the program online aligns with the competitive market. One hundred and 95.30 percent of regional and national programs, respectively, offer 100 percent distance delivery options. However, the regional programs conferring degrees may not confer a large number of degrees. This provides The Ohio State University an opportunity to secure enrollments due to a strong national brand and untapped population of potential students. The Learning House 2018 Online College Students Report indicates 75 percent of online students enroll in programs offered by institutions within 100 miles of home.

The Ohio State University's curriculum offers considerable alignment with top in-demand regional and national skills and competitor programs. Five of 17 courses display alignment with top in-demand skills such as "Intro to Operations Analytics" conferring "operating systems" and "Software Security and Reverse Engineering" conferring "software development." The Ohio State University's plan to require 26 credits for degree completion is lower than competitor offerings, potentially positioning the program as more accessible than competitors.

STATEWIDE ALTERNATIVES

(max 300 words) You are encouraged to talk with your colleagues at other institutions to learn more about their programs and discuss your unique opportunities.

1. **What programs are available in other institutions and how do they differ from the program being proposed?** *Explain the unique features of your program compared to others in the State.*

Although The Ohio State University has a great potential for cybersecurity education and training with its experts working on various aspects of cybersecurity, there are currently no other programs at bachelor's or graduate levels specializing in cybersecurity. There are a limited number of state-level alternatives offered at the professional master's level. The most recent available data dating back to 2018-2019 academic year indicates only two programs (offered by Franklin University and The University of Findlay) reported non-zero number of degree completions (14 and 10, respectively). These low numbers of degree completions (i.e., 14 and 10) suggest The Ohio State University may successfully enter the market and become a regional leader. Institution size and reputation may likely contribute to program launch opportunity.

There are also a limited number of traditional MS degrees in Cybersecurity. The closest and most relevant one is the MS in Cyber Security program offered by Wright State University, which can also be accessed online. It follows a classical MS program structure with 6 required courses, 1 elective course, and 9 credit hours of thesis work. Targeting almost exclusively students with a bachelor's degree in

computer science, this program is not well-suited for students with diverse educational backgrounds or those currently employed in the workforce, and not cross-disciplinary.

The Professional Master of Cybersecurity and Digital Trust program is a **professional** and **cross-disciplinary** master's program, which is offered **fully online**. Other online programs can also be viewed as locally significant as potential competitors. Among the top-tier competitors, the programs offered by Georgia Institute of Technology and University of Maryland can be taken exclusively online. The Georgia Tech structure requires 32 credit hours, with 9 credit hour of core courses, and offers a choice of one track out of available three. University of Maryland follows a more traditional structure with a rigid core and a number of unstructured electives, requiring 30 credit hours for matriculation. Our approach is significantly different in that the program provides students with two tracks combining the departments of Computer Science & Engineering and Electrical & Computer Engineering. It is a professional master's program, and the curriculum can accommodate working professionals' constraints.

2. Address appropriateness of specific locale for the new program.

While the program has nation-wide access through its online structure, our primary target is the Central Ohio region with its rich and diverse employment opportunities. Regional employer demand trends suggest strong need for program graduates. Across September 2017 to August 2020, employer demand for master's-level cyber security studies professionals increased 2.05 percent on average monthly, outpacing average monthly demand growth for master's-level professionals overall (i.e., 0.33 percent). This suggests graduates may enter a favorable labor market.

At a national level, national employer demand trends also suggest strong need for program graduates. From September 2017 to August 2020, employer demand for master's-level cyber security studies professionals increased 2.10 percent on average monthly, outpacing average monthly demand growth for master's-level professionals overall (i.e., 0.44 percent). This indicates students choosing to relocate after graduation will likely enter a favorable labor market as well.

3. Address opportunities for inter-institutional collaboration.

Inter-institutional collaborations are possible across the state. Due to its proximity, Wright State University can serve as a partner institution to streamline the cybersecurity specializations offered by the two universities. Further collaborations can include joint workforce education activities, open houses bringing together students and employers, and technical content development.

GROWTH OF THE PROGRAM

(max 300 words) Answers to the following questions should be consistent with the Fiscal Impact Statement in Appendix.

1. What future growth do you anticipate over several years, and how do you plan to manage this growth? When do you expect the program to be self-sufficient?

Enrollment growth: We expect to start this program with 50 students in its initial offering. The steady-state enrollment is expected to be ~150 students based on the available courses. The enrollment is expected to increase with the inclusion of subsequent topic and elective offerings, appealing to a wider audience with more diverse backgrounds and learning goals. The program is expected to be self-sufficient no later than the end of the second year of full delivery.

Due to online format, the program can handle larger class sizes more flexibly. However, additional support in teaching (e.g., additional GTAs and/or instructors) may be needed as the class sizes grow. Such growth is included in the projected budget plans.

To maximize the success of each enrolled student and graduates, the program will maintain an active self-assessment process. This will include recording of application and admission data; student academic performance indices; student evaluations of instruction (course satisfaction), semester- based student performance evaluations (reviewed by the program director and faculty committee); annual evaluations of the program by member faculty; annual student evaluations of the program; exit surveys; time-to-degree tracking; and career recording of alumni. These assessment data will be collected by the PDEP Director and staff annually and provided for review by the MCDT-GSC and used to continually refine the program. These data will also serve as support of applications seeking program funding.

Content growth: The degree includes two tracks and anticipates adding track options. Likely additional tracks are (1) *Law, Policy and Management* in conjunction with Glenn College and Moritz College and (2) one in conjunction with the Department of Integrated Systems Engineering (ISE) which would provide students content about digital trust with essential information about human factors engineering.

CURRICULUM AND INSTRUCTIONAL DESIGN

1. **Curricular content.** *Using a variation on the Table below to match your proposed program, list here all the courses that comprise the program and identify if the program will include any new courses. Include course descriptions in the Appendix for all courses that are a part of the curriculum, including those required for transcripted tracks or specializations.*

COURSE #	TITLE	CREDITS
Required core courses for degree		
IS 5195	Ethics in the Information Age	3
ECE 5561 / CSE 5471	Introduction to Cybersecurity	3
ECE or CSE 6193	Independent Studies	3
1. Design and Implementation		
ECE 5024	Introduction to Hardware Security	3
ECE 5555	Securing Autonomous Systems	3
2. Offense and Defense		
CSE 5472	Software Security	3
CSE 5194.7	Information Security	3
Elective courses (9 credits must be selected in this category)		
CSE 5473	Network Security	3
CSE 5351	Introduction to Cryptography	3
ECE 5567.01 / CSE 5477.01	Offensive Computing	3
ECE 5567.02 / CSE 5477.02	Reverse Engineering and Malware Analysis	3

All courses will be delivered online. The transition to remote instruction during the COVID-19 pandemic of 2020 and 2021, the majority of our faculty gained first-hand experience in preparing instructional material. These experiences extend to many aspects of instruction traditionally associated with in-person learning, such as laboratory sections and experiments. In computer-based practical work,

course design for online teaching is well-established. Our faculty is also well-versed in adapting classical laboratory experiments requiring access to specialized circuits and hardware using low-cost platforms that can be shipped to students (at a cost of less than \$100 per student). In other cases, students are also able to purchase the required hardware (similarly at very low cost) on their own. These experiences, combined with the ODEE's support, positions the program development on an accelerated track towards excellence.

The majority of the courses in the MCDT program are already available in various departments curricula, and new ones are approved as part of the degree requirements for other programs. Therefore, each course will be recorded and broadcast synchronously at least once a year, to accommodate students that take these courses as part of other degree requirements. All courses will be prepared for asynchronous access by students. Laboratory instructions will also be made available asynchronously. When taught exclusively asynchronously, both lectures as well as practical experiences will be paced closely by instructors. Students will have goals to achieve and have access to instructors through online office hours.

Expected Learning Outcomes and Assessment

Students who complete the degree will learn both the fundamental engineering skills (including secure circuit and autonomous system design), fundamental science skills (including cryptography and game theory) and practical skills (including reverse engineering, vulnerability discovery, malware analysis) of cybersecurity related design and implementation aspects and cyber offense and defense.

The following learning outcomes are associated with the learning goals:

a	Be familiar with policies, standards, and guidelines
b	Be familiar with cryptography algorithms
c	Be familiar with reconnaissance and various types of attacks
d	Be familiar with common software vulnerabilities and countermeasures
e	Be familiar with taxonomy of malwares and reverse engineering techniques
f	Be familiar with hardware security vulnerabilities, attacks, and countermeasures
g	Be familiar with information security threats and countermeasures
h	Be familiar with network security protocols
i	Be familiar with fundamental concepts of different real-world attacks

The students will have a good understanding to the following three questions: What is cybersecurity? Why cybersecurity is important? How to design and implement successful solutions to satisfy security needs. To understand these questions, they will be familiar with fundamental concepts of different areas in cybersecurity such as: external and internal information security threats to an organization and how to analyze and deal with them; mathematical foundations of cryptography; network security threats and countermeasures; threats and countermeasures; software vulnerabilities and countermeasures; taxonomy

of malwares and reverse engineering techniques; different real-world attacks targeted on computer systems.

Assessment Plan. The learning objectives will be reflected in exams in ECE 5561 Introduction to Cybersecurity, ECE 5024 Introduction to Hardware Security, CSE 5194.7 Information Security, and ECE or CSE 6193 Independent Studies.

2. **What are the requirements students must fulfill to complete the program successfully?** (*max 500 words*) *Expand on information in Table above, if needed including specific courses, course options and any other requirements (e.g. clinical hours, experiential learning, competencies, projects, minimal research credits, defined number of credits in different focus areas, etc). Define the minimal credits needed to complete the degree in any transcribed tracks or specializations.*

The requirements for degree completion are as follows:

- 30 semester credit hours
- Completion of the requirements from the list above

3. **Description of a required culminating, or integrated learning, experience.** (*max 500 words*).
Examples of suitable culminating experiences for different kinds of degrees include, but are not limited to: preparation of a thesis, dissertation or other creative written work; capstone or exit projects, which may be applied in nature and not necessarily involve research; comprehensive examinations; supervised field experiences, or any other integrated learning experience.

The Master of Cybersecurity and Digital Trust program achieves a balance of theoretical and hands-on learning experiences throughout the duration of study. The required courses involve significant laboratory-based experiences, which prepare the students for the workforce requirements and demands. The knowledge attained throughout the study leads to a final project-oriented Independent Study course. Sections of this course will focus on open-ended projects and be administered by different instructors focusing on different aspects of practical cybersecurity scenarios. Where applicable, those projects will include real world scenarios and projects addressing emerging trends in cybersecurity and digital trust.

INSTITUTIONAL STAFFING, FACULTY, AND STUDENT SUPPORT

1. **Faculty.** (*max 300 words*)

The courses offered in this program will be primarily taught by the faculty and instructors currently employed at The Ohio State University. The proposed program includes a number of courses that have already been offered multiple times, augmented with additional courses that have been approved for offering in partnering departments. These courses are expected to be taught mainly by tenure-track faculty and full-time instructors. Two of the courses in the program will be taught by the domain experts currently employed at our industry partner Battelle. An agreement between OSU and Battelle is being finalized.

We anticipate a total of 10 faculty members will be involved in the program, and no new faculty lines will be needed to maintain the program going forward. If tracks are added to the program, the number of faculty members associated with the program will increase, as well. With the anticipated growth in the number of tracks, we project an increased load in the Independent Studies course, which will require the hiring of a full-time instructor supervising the final projects.

2. **Administration and Support.** (*max 300 words*) *What are the administrative arrangements for the*

proposed program, including oversight at the program, department and school/college level? Where will any needed financial support and staffing come from?

Faculty Director

The MCDT Faculty Director will be selected by the MCDT Graduate Studies Committee. The MCDT Faculty Director will have graduate faculty status with the Graduate School and strong affiliation with ICDT.

Administrative Staff

The Director of Professional and Distance Education Programs (PDEP) who reports to the Dean of the College of Engineering, will act as the MCDT Administrative Director. The existing PDEP staff including an Assistant Director and Program Coordinator for Degrees will manage the day-to-day operations, processing of applications and coordination with the MCDT-GSC and provide student advising and support. The PDEP marketing specialist will provide program marketing of the degree.

Master Engineering Management – Graduate Studies Committee (MCDT-GSC)

All voting members of the MCDT-GSC will have graduate faculty status with the Graduate School. The MCDT-GSC will handle all tasks normally associated with a graduate studies committee (admissions, new courses, monitoring progress of students, and so on).

Financial Support

The College of Engineering financially supports PDEP and values the future MCDT. Both the Departments of CSE and ECE are also behind the roll out of this new degree, working to bootstrap the cost of faculty to teach the first few semesters, with anticipation of growing enrollments where tuition revenue will eventually meet and exceed the expenses required. Examples of the financial creativity includes time sharing administrative staff, offering supplemental pay for faculty overload, and gradually increasing the course offering schedule. All parties understand there will be a loss before there is a gain.

ADDITIONAL PROPOSAL SECTIONS FOR ENTRY LEVEL GRADUATE PROGRAMS, PROFESSIONAL GRADUATE PROGRAMS, AND PROFESSIONAL SCIENCE MASTERS

The following three sections are not needed for all program proposals, but you must complete the relevant sections if they apply to your program. Delete the sections that are not relevant for your proposal.

PROFESSIONAL GRADUATE DEGREE PROGRAMS

- a) *What admission criteria, in addition to the traditionally required transcripts, standardized test scores, letter(s) of recommendation, and personal statements of purpose, are relevant to assess the potential for academic and professional success of prospective students? Will there be special consideration of student experience and extant practical skills within the admission process? If so, please elaborate.*

The MCDT program is a professional master's program. While a Bachelor's degree is required for admission, the expectation is to focus on the relevance of the applicants' experience to the degree requirements. This information will be clearly communicated to the applicants. Moreover, a significant share of the program's attendees will be recruited from the workforce directly. Therefore, professional experiences, positions they hold in the industry, and any existing professional certificates will be included in their admission assessment. A combination of applicants' professional experiences,

academic credentials, statements of purpose, and letters of recommendation will be used in a holistic evaluation process to assess their suitability to the program composition and their future career prospects.

- b) *Is field/clinical experience subsumed within the academic experience? If so, how does that experience relate to the academic goals of the professional graduate degree program? Provide a description of the involvement of supervisory personnel. Describe the nature of the oversight of the field/clinical experience by the academic department. Provide an outline of the anticipated student activities as well as student requirements for competencies and hours of experience.*

N/A

- c) *Are the faculty qualifications associated with the professional graduate degree program appropriate for such faculty? Provide the specific qualifications for such faculty.*

The proposed professional degree program has both theoretical as well as practice-oriented components. The expertise required to run both aspects are already prerequisites for tenure-track faculty employed at The Ohio State University. Additional instructional support from our industry partners are assessed with their professional experiences as well as their prior teaching experiences in other training and education programs.

- d) *How does accreditation by the appropriate professional organization relate to the academic curriculum and experience outlined in the program plan? Describe the specific aspects of the program plan, if any, that are necessary to achieve professional accreditation. Is completion of the degree program required for professional accreditation in the field?*

The tracks that make up the program has been informed by the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework developed by the National Institute of Standards and Technology (part of U.S. Department of Commerce). While the graduates of the program will be well-prepared for accreditation programs based on the NICE framework, accreditation is not an explicit or immediate goal of MCDT.

- e) *How are theory and practice integrated within the curriculum?*

The courses are designed to integrate both didactic instruction as well as hands-on/practical experiences. The program also includes a final project-oriented course where all topical contents are put to use to solve an open-ended, real-life-inspired problems in a team setting.

- f) *What is the national credit hour norm for this degree program in your field? How was this norm derived? Is the number of credit hours required for graduation influenced by mandated professional experiences? If so, how?*

Our market research revealed that 30 credit hours of work is typical for professional master's degree programs focusing on cybersecurity and other related topics. This number is generally not influenced by any mandated professional experiences.

- g) *Describe how the required culminating academic experience will contribute to the enhancement of the student's professional preparation.*

The culminating academic experience will allow the students to view the cybersecurity and digital trust topics from a wider vantage point. In practice, professionals employed in cybersecurity and digital trust positions have a narrow field of expertise, which is known to inhibit their ability to assess multi-faceted nature of complex cybersecurity problems. The MCDT program provides the breadth required to

appreciate, identify, and act on the aforementioned complexity and the interdependence of multiple problem instances in the workplace. The depth conveyed in each track prepares the students to tackle these complex problems at an expert level. As the MCDT program requires the completion of two such tracks, the graduates will be ready for employment with larger number of prospects, preparing them for future professional growth and advancement opportunities.

FACULTY MATRIX

A faculty member must be identified for each course that is a required component of the curriculum. If a faculty member has not yet been identified for a course, indicate that as an “open position” and describe the necessary minimum qualifications in the matrix (as shown in the example below). **All program proposals must include both the Faculty Matrix and a copy of each faculty member’s 2-page CV as Appendix items.**

Instructor Name	Rank or Title	Full-Time (FT) or Part-Time (PT)	Instructor Qualification			Courses taught in the proposed program (Include course number and title)
			Degree Title, Discipline Institution, Year	Years of Teaching Experience In the Discipline/ Field	Additional qualifications (e.g., licenses, certifications)	
Zhiqiang LIN	Distinguished Professor of Engineering	FT	PhD. Computer Science, Purdue University, 2011	12		CSE 5474: Software Security
Irem ERYILMAZ	Assistant Professor	FT	PhD. Electrical and Computer Engineering, 2016			CSE 5471 / ECE 5561: Introduction to Cybersecurity
Carter YAGEMANN	Assistant Professor	FT	PhD. Computer Science, Georgia Institute of Technology, 2022	2		CSE 5472: Information Security Projects CSE 5477.02 / ECE 5567.02: Reverse Engineering & Malware Analysis CSE 5477.01 / ECE 5567.01: Offensive Security
Waleed KHALIL	Professor	FT	PhD. RFICs , Arizona State University, 2008	14		ECE 5024: Introduction to Hardware Security
Shailesh Bojja Venkatakrishnan	Assistant Professor	FT	PhD. Electrical and Computer Engineering, University of Illinois Urbana-Champaign, 2017	6		CSE 5473: Network Security
Steve LAI	Professor	FT		40		CSE 5351: Introduction to Cryptography
Open Position		FT or PT				ECE 5555: Securing Autonomous Systems

ADEMDUM – follow-up to CCAA discussions on December 4, 2023, of the importance of including human factors in a program to educate students about cybersecurity and digital trust.

It is essential that all engineering professionals recognize that cyberspace is a sociotechnical system, or rather a system of systems. The term “sociotechnical system” refers to systems that include technical elements (including hardware and software components) and social elements (people and contextual environments); both these major subsystems, the technical and the social, should be equally valued and attended to in the effort to create 'trustworthy' digital systems. “The characterization of human factors, which includes human behavior, is needed to understand how the actions of users, defenders, and attackers affect cyber security risk” (Henshel et al. 2015). It is essential that designers and engineers working in the area of cybersecurity are educated to understand that humans in the system are not simply vulnerabilities and risk elements in cyberspace and that the best cybersecurity designs are informed by knowledge of human factors. Any educational or training program teaching students about digital trust should include human factors engineering as a required element.

Security is a human endeavor, in which we have built increasingly sophisticated and complex tooling and structures to help us secure sophisticated and complex systems that are increasingly digital. As the digital medium is inherently synthetic and inherently opaque, all functions and features need to be explicitly designed and implemented to support and augment the people in the system. Two of the human roles in particular that should be highlighted in this educational program for explicit support are 1) the designer of the cyberinfrastructure and 2) the analyst that must monitor the infrastructure after implementation. We must help designers understand how to build their solutions as reliably as possible with minimal vulnerabilities, but also ensure they know that these engineered systems will never be perfectly reliable or without vulnerabilities. As such, these same technologies must be designed and engineered to be “good team players”, which means that they will be observable, predictable, and directable to and with their human counterparts. In this way, the designers' work will actively and intentionally support the analysts. This requires making tradeoff decisions due to finite budgets and resource availabilities on prioritizing the patches and other preventative measures that keep the system safe, and it also requires that the system be designed to enable and facilitate analysts to investigate and mitigate active threats. Other human roles that must be supported are those of the rank and file employees or members of that system. These users can be targeted as vulnerabilities or be a source of security. How does the overall system, including the technological tools, business processes and overall organizational design, support the tradeoffs made everyday between defending the system today and fortifying it for tomorrow? Courses in the Department of Integrated Systems Engineering (ISE) that would provide students learning about digital trust with essential information about human factors engineering are the following:

1. ISE 5700: Introduction to Cognitive Systems Engineering
2. ISE 5760: Visual Analytics for Sensemaking
3. ISE 5770: Cognitive Engineering Design
4. ISE 5870: Resilience Engineering

Reference:

Henshel, D., Cains, M.G., Hoffman, B., Kelley, T., 2015. Trust as a Human Factor in Holistic Cyber Security Risk Assessment,. *Procedia Manufacturing* 3, 1117-1124.

Additional suggested reading:

Venables, Adrian. (2021). Modelling Cyberspace to Determine Cybersecurity Training Requirements *Frontiers in Education* 6. doi: DOI=10.3389/feduc.2021.768037



Student Name:

First Middle Initial Last

OSU ID#

OSU Email Address:

Phone:

Advisor:

Required Core Courses (9 cr hrs)

Course Number	Course Name	Credit Hrs	Term/Year
IS 5195	Ethics in the Information Age	3	
ECE or CSE 6193	Independent Studies	3	
ECE 5561 or CSE 5471	Introduction to Cybersecurity	3	

First Semester Enrolled:

☐ Autumn

☐ Spring

Year: _____

Required courses Design and Implementation (6 cr hrs)

ECE 5024	Introduction to Hardware Security	3	
ECE 5555	Securing Autonomous Systems	3	

Projected Graduation:

☐ Autumn

☐ Spring

Year: _____

Required courses Offense and Defense (6 cr hrs)

CSE 5472	Information Security Projects	3	
CSE 5474	Software Security	3	

Elective courses (9 cr hrs)

ECE or CSE 5567.01	Offensive Security	3	
ECE or CSE 5567.02	Reverse Engineering & Malware Analysis	3	
CSE 5473	Network Security	3	
CSE 5351	Introduction to Cryptography	3	

Total Degree Credit Hours: _____

Must be a minimum of 30

Date: _____

Student Signature: _____

Advisor Signature: _____



**THE OHIO STATE
UNIVERSITY**

Curriculum Proposal Checklist

Title of Program:

Effective term:

College:

New/Establish:

Secondary Major Eligible:

Academic Unit:

Revise:

50% Revision:

Mark Up:

Program Contact:

Terminate:

Suspend:

Certificate Category*:

Degree/Credential:

Program of Study :

Title:

Code:

Program Focus*:

Credit hours to degree/credential:

Is this a change to the current total?

Yes No

Program offered only online?

Yes No

If yes, is there a signed MOU with ODEE?

Yes No

Campus(es) where offered:

Columbus

ATI

Lima

Mansfield

Marion

Newark

Rationale:

Student Curriculum Sheet Required:

Four Year (or appropriate) Plan:

Academic Unit Curriculum Committee approval date:

College Curriculum Committee approval date:

Graduate School Council approval date*:

Regional Campus approval date*:

Council on Academic Affairs approval date:

University Senate approval date*:

Board of Trustees approval date*:

ODHE approval date*:

*** If applicable**