THE OHIO STATE UNIVERSITY

College of Engineering

Undergraduate Education & Student Services

122 Hitchcock Hall
2070 Neil Avenue
Columbus, OH 43210-1278

614-292-2651 Phone
614-292-9379 Fax

engineering.osu.edu

Memo

To: Randy Smith, Vice Provost for Academic Programs
From: Rosie Quinzon-Bonello, Assistant Dean for Curriculum and Assessment
Date: December 9, 2024
Re: Institute for Cybersecurity and Digital Trust

Attached is a proposal submitted by the College of Engineering to formally establish the Institute for Cybersecurity and Digital Trust (ICDT) as a college-level center.

This proposal provides the institute's

- background, mission, vision, and brief history
- delegation of academic responsibility and administration

Not in included in the proposal but also requested is to retain "Institute" in the name. This is for consistency and to avoid any confusion that may arise should "Institute" be replaced with "Center."

On December 5, 2024, the College of Engineering Committee for Academic Affairs approved the proposal. Please let me know if you require additional information.

Sincerely,

Rosie Quinzon-Bonello

Institute for Cybersecurity and Digital Trust

Ayanna Howard, Dean
College of Engineering
October 2024

(Contacts for review: Zhiqiang Lin.3021, Julia Armstrong.798, or David Tomasko.1)

The College of Engineering proposes to formally establish the Institute for Cybersecurity and Digital Trust (ICDT) as a College-level Center. As will be explained below, the Center was originally envisioned as a university-level institute and was given provisional status to operate as such in 2019. The pandemic and turnover in university and program leadership prompted a re-evaluation to recast the ICDT as a college-level center. This brief description and justification is provided as notification to the Office of Academic Affairs and the Council on Academic Affairs of our intent to do so under our own pattern of administration. Because the College plans to delegate authority to ICDT to deliver for-credit courses and programs, this short proposal is being submitted to the appropriate academic review committees for review in accordance with Appendix B of the College of Engineering pattern of administration (see Appendix I for relevant policy).

Background

In practice, Cybersecurity is a group of disciplines that seek to understand how the combination of people, technologies and data interact to introduce cyber risk, and how individuals and organizations make choices regarding management of those risks. Components of trust in the digital age include competence, benevolence, honesty, predictability, and non-opportunism. Cybersecurity principles of privacy, confidentiality, availability and integrity operationalize these elements. For the Institute, Digital Trust is the study of the interactions between those who guarantee trust, and those who expect to be able to trust, in the digital world.

ICDT's mission is to:

· Foster collaboration among researchers from multiple academic disciplines to collaboratively develop solutions to complex cybersecurity and digital trust issues.

· Prepare the next generation of workers, scholars and leaders to develop robust and effective cyber trust solutions.

· Partner with other educational institutions, government, military and industry to identify emerging cybersecurity issues and find ways to address those needs through research, education and collaboration.

The Vision is:

Ensuring that Ohio State provides a scientific, cross-disciplinary focus for academics and the Ohio State community to explore cybersecurity issues related to hardware, software and human elements, and digital trust issues through the lenses of technology, behavior, attitudes, context, and experience.

Brief history

Originally, a proposal was prepared by a group of faculty and university staff from the Department of Computer Science and Engineering, Department of Electrical and Computer Engineering, and the Chief Information Security Officer in the Office of Technology and Digital Innovation. The establishment of ICDT gained provisional approval by the university around 2018 and it began developing programming, outreach, and sponsored research in the area. Currently it is operational with a Faculty Director (ZQ Lin), Managing Director (Julia Armstrong), and two Associate Directors (Ted Allen, Roland Kreml), see https://icdt.osu.edu/.

Due to leadership changes at both the College and University level and the pandemic, the Institute was never formalized at the university level. In 2022, new College leadership agreed to support and manage ICDT exclusively as a *college research center* in the College of Engineering. Given the need to meet the JobsOhio requirement to create an MS in Cybersecurity, alongside other research and teaching initiatives, Dean Howard made the decision for Engineering to oversee ICDT's activities. As a result, all institutional support currently comes from Engineering's strategic funds as the center scales to a sustainable model.

A brief list of current educational, research, and outreach activities already being carried out by ICDT is provided in Appendix II.

Delegation of Academic Responsibility

Due to the importance of the subject matter and the existence of curricular programs, the College desires to delegate to ICDT the authority to develop and deliver for-credit courses and programs in the areas of Cybersecurity and Digital Trust. This includes the previously approved graduate certificates in *Cybersecurity Design and Implementation* and *Cybersecurity Offense and Defense*. It also includes the upcoming *Master of Science in Cybersecurity and Digital Trust* that builds upon the existing certificates. ICDT would also have authority to bring forward additional programs as needs are identified.

In carrying out academic efforts, ICDT is expected to collaborate with existing units as any other program would. Development of courses and programs is subject to concurrence from relevant stakeholders following established academic review practices.

Administration

As indicated in the history, the College supports and manages the center through its strategic funds. The Faculty Director is appointed by and accountable to the Dean of the College and appointed at their discretion. After a start up period, ICDT is expected to move into engineering research operations and have a sustainable business model to support its activities.

Appendix I – College of Engineering Pattern of Administration

Relevant language from Appendix B:

College Centers will generally not offer for-credit courses or degree programs, but such offering may be allowed in certain cases. If the center proposes to offer for-credit or degree programs, the proposal must also be reviewed by the College Committee on Academic Affairs, and will require approval by both the College faculty and the Council on Academic Affairs (see Faculty Rule 3335-3-36). Prior to review by the College faculty, the College Committee on Academic Affairs shall review and make a recommendation on such courses or degree programs.

Appendix II – Brief list of ICDT recent activities (FY25)

1. Professional Affiliations with Active ICDT Engagement
    a. National Security Administration's National Centers of Academic Excellence
        i. 5-year designation in Cyber Defense for the CSE ICA Program of Study
        ii. Application in progress for a Research designation
    b. US CYBERCOM Academic Engagement Network
    c. Griffiths' Institute VICEROY Program
        i. Midwest VICEROY Institute (MVI) with Univ. of Kansas and Purdue Northwest
        ii. Scholarships for students to learn outside of the regular curriculum
    d. Ohio Cyber Collaboration Committee (OC3) for the Adjutant General
        i. Active on the Education and Workforce subcommittee
    e. Ohio Cyber Range Institute (OCRI)
        i. Regional Programming Center for OCRI
        ii. Host for Ohio Cyber Reserve's Ohio Cyber Guardian event in 2024
2. Research Progress
    a. Proposals flagged with ICDT now total over $14M since 2022
    b. Awards received flagged with ICDT now total over $7M since 2022
    c. Sponsors include ARO, DARPA, NSA, NSF, ODHE, ONR, TRC, and several companies (e.g., Cisco, Aptive, Amazon, Meta, and Vmware) and research centers.
    d. Lead PIs are all within the College of Engineering
    e. Research results won best paper awards from
        i. 2024 IEEE Symposium on Security and Privacy (S&P'24)
        ii. 2023 International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (SMARTSP'23)
        iii. (Honorable Mention) 2022 ACM Conference on Computer and Communications Security (CCS'22)
    f. Artifact won distinguished artifact award from
        i. 2024 Network and Distributed Security Symposium (NDSS'24).
3. Curricular Growth for Ohio State
    a. New online Masters in Cybersecurity and Digital Trust
    b. Online masters-level certificates in Design & Implementation, Offense & Defense
    c. Collaboration with 2-yr colleges for students with an AAS in Cybersecurity to complete a bachelor's degree at Ohio State
    d. Potential to propose and support a new 4-Credit Hour General Education course in the Citizenship for a Diverse World theme, with service-learning component
    e. Working towards College Credit Plus course offerings with local high schools
4. Student Support at Ohio State
    a. Support for several student organizations (Women in Cybersecurity chapter, Cybersecurity Club, Embedded Security Club)
    b. Support for students to enter competitions (MITRE, NSA's Codebreaker Challenge, RECon research paper competition, etc)
    c. MVI Scholarships for students to prepare for certification exams or undergraduate research experiences

    d. Continual communication on scholarships, internships and job opportunities
5. Community Engagement on and off campus
    a. Hosting speaker series in person and online for campus community and beyond
    b. Annual Research Symposium
    c. Annual Industry Symposium
    d. Support for Mansfield & Richland Co.'s monthly community series
    e. Partnerships on campus with other institutions such as Center for Design and Manufacturing Excellence, Translational Data Analytics Institute, The Battelle Center for Science, Engineering and Public Policy.