From:	Smith, Randy
To:	Greenbaum, Rob; Armstrong, Julia
Cc:	Williams, Valarie; Smith, Randy; Griffiths, Rob; Miriti, Maria; Reed, Katie; Duffy, Lisa; Hunt, Ryan; Matyas, Cory; Tomasko, David; Shanker, Balasubramaniam; Moulton, Stephanie; Simmons, Ric; Barnett, Kent; Hammond, Ivy; Watson, Sara; Schoon, Eric; Talbot, Ann; Warren, Adam; Eveland, Jessica; Brown, Trevor
Subject:	Proposal to establish a new track in Law, Policy and Management to the Master of Cybersecurity and Digital Trust
Date:	Friday, October 23, 2026 4:25:28 PM
Attachments:	image001.png

Julia and Rob:

The proposal from the John Glenn College of Public Affairs, the College of Engineering, and the Moritz College of Law to establish a new track in Law, Policy and Management to the Master of Cybersecurity and Digital Trust Medicine was approved by the Council on Academic Affairs at its meeting on October 21, 2026. 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 **November 19, 2026**. 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 **November 5, 2026,** and the Senate Steering Committee on **November 6, 2026**. 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 **December 3, 2026.** If approved by the Board, the Graduate School will work with you on the approval process with the Ohio Department of Higher Education.

Once fully approved, the Office of the University Registrar will work with you on 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 Valarie Williams(.1415), or me.

I wish you success with this important program development.

Randy

THE OHIO STATE UNIVERSITY

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

TO: Randy Smith, Vice Provost for Academic Programs

FROM: Graduate School Curriculum Services

DATE: 10/1/2026

RE: Proposal to Establish a New Track in Law, Policy and Management in the Master of Cybersecurity and Digital Trust in The College of Engineering

The Institute for Cybersecurity and Digital Trust in the College of Engineering is proposing a New Track in Law, Policy and Management.

The proposal was received by the Graduate School on 7/08/2026. The combined GS/CAA subcommittee first reviewed the proposal on 9/23/2026 and requested revisions. Revisions were received on 10/1/2026. It is supported for review by the Council on Academic Affairs.

THE OHIO STATE UNIVERSITY

College of Engineering

Institute for Cybersecurity & Digital Trust

395 Dreese Labs
2015 Neil Avenue
Columbus, OH 43210
614-688-1909 Phone

icdt.osu.edu

September 29, 2026

Graduate School – Council on Academic Affairs (GS/CAA)
Review Committee

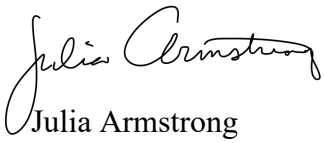
Letter of Addendum

In regards to Lisa Kowalsky's email on September 24, 2026, we would like to respond to your request on "a statement of projected student interest and established specializations."

> Interest has already been expressed by students in cybersecurity and computing disciplines who seek a deeper understanding of governance, regulatory frameworks, risk, privacy, and compliance. However, the larger audience is likely to be students pursuing interdisciplinary pathways that connect technology with public policy, legal studies, and organizational leadership. Because many cybersecurity roles do not require advanced software development skills, this track expands access to cybersecurity career opportunities beyond software security. In addition, prospective students are increasingly interested in careers within regulated industries and the public sector, where legal and policy awareness is essential. Collectively, these indicators suggest sustained demand for a track that integrates technical foundations with legal and policy perspectives, preparing graduates for roles that require both cybersecurity expertise and an understanding of broader institutional and regulatory environments.

The College of Engineering is proud to support this additional curricular pathway to the established Masters of Cybersecurity and Digital Trust.

Sincerely,



Julia Armstrong
Executive Director
Institute for Cybersecurity and Digital Trust
Armstrong.798@osu.edu

To: grad-schoolcurriculum@osu.edu
Subject: Proposal

Hello,
The Master of Cybersecurity and Digital Trust proposes to add a Law, Policy, and Management track. This proposal was reviewed and unanimously approved today at Engineering's College Committee on Academic Affairs.

I am attaching the full proposal for Graduate School review. Please let me know if any other information would be helpful.

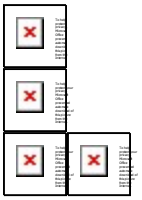
Thank you!
Cory

THE OHIO STATE UNIV

Corinne Matyas
Assistant Dean of Curriculum and Assessment
College of Engineering
117 Hitchcock Hall | 2070 Neil Ave. | Columbus, OH 43210
614-292-2154 | matyas.3@osu.edu



thread::duq959H6DWin2dqyar7q4R4::



Docusign Envelope ID: 7F68B557-65C3-8C0E-8239-8B98A86DD6D0

THE OHIO STATE UNIVERSITY

John Glenn College of Public Affairs

110 Page Hall
1810 College Road
Columbus, OH 43210
glenn.osu.edu

July 2, 2026

Mary Stromberger
Vice Provost for Graduate Education and Dean of the Graduate School
250 University Hall
230 N. Oval Mall
Columbus, OH 43210

Dear Dr. Stromberger:

The John Glenn College of Public Affairs provides full and enthusiast support for the addition of a Law, Policy, and Management track to the new Master of Cybersecurity and Digital Trust degree.

From the early discussions about the idea of this new degree, the Glenn and Moritz colleges were encouraged to develop law and policy coursework to contribute to the degree. This proposed additional track fulfills that contribution. Our college's graduate studies curriculum committee voted to approve the proposed new track on September 12, 2024.

The addition of this new track option will be attractive to graduates needing to better understand the legal and policy implications of cybersecurity. The track fills an important gap in addressing the need to train public, nonprofit, and private sector managers about the institutions governing cybersecurity policy. Federal and state law and policy provide the foundational formal rules for cybersecurity governance systems. Managers must understand these rules as they develop organizational policy and managerial strategies. Technicians, policymakers, and managers must understand the legal mandates they should follow and must understand how to implement these mandates using socio-technical solutions to manage cybersecurity threats.

The colleges of Engineering, Law, and Public Affairs are already successfully collaborating on a new graduate certificate in Cybersecurity Law, Policy, and Management, and this certificate has had strong student interest in its first year. We are hopeful that the proposed new track in the Master of Cybersecurity and Digital Trust degree, based on some of the same courses, will likewise increase interest in the new master's degree.

Sincerely,

DocuSigned by:
Stephanie Moulton
5EDDA5CAE2C54FE...

Stephanie Moulton
Acting Dean & Professor, John Glenn College of Public Affairs
300 Page Hall
Moulton.23@osu.edu

From: Simmons, Ric simmons.239@osu.edu
Sent: Thursday, July 2, 2026 2:05 PM
To: Greenbaum, Rob greenbaum.3@osu.edu
Subject: Re: MCDT addition of Law and Policy

The Moritz College of Law fully supports the addition of a Law, Policy, and Management track to the new Master of Cybersecurity and Digital Trust degree. The new track will be a useful addition to the degree, and it will enhance the successful collaboration between the colleges of Law, Engineering, and Public Affairs.

Ric Simmons
Associate Dean for Academic Affairs and Strategic Initiatives
Jacob E. Davis and Jacob E. Davis II Chair in Law
Moritz College of Law
The Ohio State University

Proposal to Add a Law, Policy, and Management track to the Master of Cybersecurity and Digital Trust Degree

The John Glenn College of Public Affairs and the Moritz College of Law propose to add an additional track, Law, Policy, and Management, to the new Master of Cybersecurity and Digital Trust (MCDT) degree. From the time the idea of a new degree built on stackable certificates was proposed, the Glenn and Moritz colleges were encouraged to develop law and policy coursework to contribute to the degree. The approved MCDT proposal anticipated the addition of new tracts:

> **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.

In response to the ask, we have created a proposed new graduate certificate and specialization in the Glenn College's Master of Public Administration and Leadership (MPAL) degree. Based on that curriculum, we propose the following new MCDT track. We believe that the addition of this new track option will be attractive to graduates who need to better understand the legal and policy implications of cybersecurity. The track maps directly into program learning goal A: Be familiar with policies, standards, and guidelines.

This track will fill an important gap in addressing the need to train public, nonprofit, and private sector managers about the institutions that currently govern cybersecurity policy. Federal and state law and policy provide the foundational formal rules for cybersecurity governance systems. Managers must understand these rules as they develop organizational policy and managerial strategies. While cybersecurity threats begin with information and communications technology, the solutions are more than "technical." For many experts in the field, the most significant cybersecurity threats are not technical in nature but are caused by human error. Technicians, policymakers, and managers must understand the legal mandates they should follow and understand how to implement these mandates using socio-technical solutions to manage the cybersecurity threats posed by human error.

Coursework

3. Law, Policy, and Management
Two required classes
LAW 7805 Data Privacy, Cyber Security Regulation and Compliance
PUBAFRS 5510 Cybersecurity Law, Management, and Policy

Additionally, we recommend adding the following elective course offerings
LAW 7804 Law of Cyberspace
PUBAFRS 5570 Data & Information Governance
PUBAFRS 7600 Federal Policy and Management

Given that the current construction of the degree requires students to take 9 credit hours of electives, we also recommend that students be provided with the option to use those elective hours to enroll in a third transcriptable track. For students not choosing to do so, we further recommend allowing students to utilize any core courses in the track(s) they do not pursue as electives.

The following table illustrates the revised degree curriculum with the proposed new track and elective courses in red.

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
	3. Law, Policy, and Management	
LAW 7805	Data Privacy, Cyber Security Regulation and Compliance	3
PUBAFRS 5510	Cybersecurity Law, Management, and Policy	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
LAW 7804	Law of Cyberspace	3
PUBAFRS 5570	Data & Information Governance	3
PUBAFRS 7600	Federal Policy and Management	3

Short Course Descriptions

Law of Cyberspace (7804): This course allows students with varying backgrounds to confront the cutting-edge legal issues that arise from technological change and the Internet.

Data Privacy and Cyber Security Regulation and Compliance (7805): This course examines the legal, policy, and operational management issues related to data privacy and data protection. Privacy and cybersecurity law is a rapidly developing area of law as governments, businesses and society respond to the growing challenges and risks associated with protecting individual privacy in a digital world. Data privacy law affects a vast range of businesses, products, and processes, including social media, marketing, healthcare, manufacturing, finance, retail, and technology. This course reviews U.S. federal and state law and regulations in depth and provides an overview of the EU General Data Protection Regulation (GDPR) and other global data protection schemes. It adopts an operational approach that focuses on a privacy lawyer or privacy professional's role within the corporate environment, touching on the various aspects a data privacy function has on legal and compliance, information technology, marketing, human resources, information security, and internal audit. Students will learn to apply privacy and cybersecurity legal frameworks across sectors and to assess regulatory requirements through course readings, discussions, guest lecturers, and assignments, which will include working through real world scenarios such as responding to a data breach and developing a privacy policy.

Cybersecurity Law, Policy and Management (5510): This course provides an integrated focus on the making and implementing of cybersecurity policy, while exploring the interaction of technology, law, policy, and management. The class aims to equip policymakers in the cybersecurity realm with legal, policy, and managerial concepts and tools to effectively deter cyber threats.

Data and Information Governance (5570): This class focuses on data governance with an emphasis on cybersecurity. It covers risk management, data security, information quality, and data modeling. Students engage in case studies and simulations to apply concepts, preparing them to manage data effectively in public, private, and non-profit sectors. The curriculum also includes discussions on ethical considerations and regulatory compliance. Students should have prior experience with conducting data analysis. At least junior undergraduate status is strongly suggested. Students are encouraged to contact the instructor if they have concerns about their level of preparation.