From:	Smith, Randy
То:	Ralph, Anne; Landsbergen, David; Greenbaum, Rob
Cc:	Sutherland, Sue; Reed, Katie; Smith, Randy; Griffiths, Rob; Miriti, Maria; Duffy, Lisa; Hunt, Ryan; Brown, Trevor; Barnett, Kent
Subject:	Proposal to establish a Graduate Certificate (type 3a and 3b) in Cybersecurity, Law, Policy, and Management
Date:	Thursday, May 29, 2025 4:15:48 PM
Attachments:	image001.png

Anne, David, and Rob:

The proposal from the John Glenn College of Public Affairs and the Moritz College of Law to establish a Graduate Certificate (type 3a and 3b) in Cybersecurity, Law, Policy, and Management was approved by the Council on Academic Affairs at its meeting on May 28, 2025. Thank you for attending the meeting to respond to questions/comments.

No additional level of internal review/approval is necessary. This action will be included in the Council's next <u>Annual Activities Report</u> to the University Senate (July 2025).

The Office of the University Registrar will work with 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 Sue Sutherland (.43), 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: <u>4/29/2025</u>

RE: Proposal to Establish a New 3a & 3b Graduate Certificate in Cybersecurity Policy, Law and Management in The John Glenn College of Public Affairs and the Moritz College of Law.

The John Glenn College of Public Affairs in collaboration with the Moritz College of Law is proposing a New 3a & 3b Graduate Certificate in Cybersecurity Policy, Law and Management.

The proposal was received by the Graduate School on $\frac{4/18/2025}{4/24/2025}$. The combined GS/CAA subcommittee first reviewed the proposal on $\frac{4/24/2025}{4/24/2025}$ and support its review by the Council on Academic Affairs.

Proposal for Type 3a and 3b Graduate Certificate in Cybersecurity Law, Policy, and Management

The John Glenn College of Public Affairs The Moritz College of Law

Table of Contents

- 1. Letter from Associate Dean for Curriculum Dr. Robert Greenbaum
- 2. Letter from Graduate Studies Director Dr. James Landers
- 3. Letter of support from Moritz
- 4. Letter of support from College of Engineering
- 5. Proposal in Cybersecurity Law, Policy, and Management
 - a. Program Overview
 - b. Rationale
 - c. Certificate Objectives
 - d. Market Assessment
 - i. Market Demand
 - ii. Market Supply
 - e. Curriculum
 - f. Assessment
 - g. Eligibility
 - h. Administrative Support
 - i. Marketing
 - ii. Recruitment and Admissions
 - iii. Advising and Student Support
 - iv. Tuition and Student Fees
 - i. Planned Enrollment
- 6. Curriculum Proposal Checklist
- 7. OSO Memorandum of Understanding
- 8. Appendices
 - a. Course Syllabi
 - i. ECE 5561: Introduction to Cybersecurity
 - ii. PUBAFRS 5510: Cybersecurity Law, Policy, and Management
 - iii. PUBAFRS 5570: Data and Information Governance
 - iv. LAW 7805: Data Privacy, Cyber Security Regulation and Compliance
 - v. LAW 7804: Law of Cyberspace
 - b. Market feasibility study completed by OSO
 - c. Additional List of cybersecurity curricular offerings in Ohio



John Glenn College of Public Affairs

Robert T. Greenbaum Associate Dean for Curriculum

> 350E Page Hall 1810 College Road Columbus, OH 43210 614-292-9578 greenbaum.3@osu.edu glenn.osu.edu

April 3, 2025

Vice Provost W. Randy Smith Council on Academic Affairs Office of Academic Affairs

Dear Randy:

Please find enclosed a proposal and supporting documentation for a new Type 3a Stand Alone and 3b Embedded Graduate Certificate in Cybersecurity Law, Policy, and Management (CLPM). This 15-credithour online certificate represents a collaboration between the Glenn College, Moritz College, and the College of Engineering.

The CLPM certificate fills an important gap in addressing the need to train public, nonprofit, and private sector managers about the institutions governing cybersecurity policy. Because cybersecurity is a public good, it must be collectively governed by the public, nonprofit, and private sectors. Federal and state law and policy provide the foundational formal rules for these governance systems. Managers must understand these rules as they develop organizational policy and managerial strategies.

Cyber attacks have been increasing in intensity, and employers both nationally and in Oho have been responding by posting increasing numbers of cybersecurity jobs. This certificate should be popular both as a standalone certificate for managers who need specialized training in cybersecurity and for current students looking to add a credential in a growing field.

John Glenn College of Public Affairs Graduate Studies Committee voted unanimously to approve the proposal on January 12, 2024. The proposal was presented to the Glenn College faculty at its May 10, 2024, faculty/staff meeting. After the meeting, the faculty voted online 22-1 to approve the proposal.

The Glenn College's Graduate Studies Committee subsequently voted on September 12, 2024, to utilize this coursework to propose to the College of Engineering a Cybersecurity Law, Policy, and Management track in the new Master of Cybersecurity and Digital Trust degree (creating a third track option) and to create a Cybersecurity Law, Policy, and Management Specialization in the Glenn College's Master of Public Administration and Management (MPAL) degree (creating a fifth specialization option).



We are separately submitting our proposal to add the new specialization to the MPAL degree, and the proposed new track will come through the College of Engineering.

We look forward to your review of the proposal.

Sincerely,

Rob Theenbaum

Robert T. Greenbaum Professor



May 14, 2024

Dr. Mary Stromberger, PhD Vice Provost for Graduate Education and Dean of the Graduate School 250 University Hall 320 N. Oval Mall Columbus, OH 43210

Dear Dr. Stromberger:

I am writing to inform you that on January 12, 2024, the Glenn College Graduate Studies Committee voted unanimously to move forward with the proposal for a new stand-alone certificate in Cybersecurity Law, Policy, and Management.

The committee believes that the certificate will help fill the increasing demand for cybersecurity expertise in the public, private, and nonprofit sectors and provide significant benefits to the community, state, and nation.

Sincerely,

Jane & Londen

James R. Landers Associate Professor of Practice in Public Affairs, Enarson Fellow Director of Graduate Professional Studies 210B Page Hall, 1810 College Rd, Columbus OH 43210 Email: landers.1@osu.edu



Anne E. Ralph Associate Dean for Academic Affairs & Strategic Initiatives Morgan E. Shipman Professor in Law Tel: 614-247-4797 Email: ralph.52@osu.edu

Robert T. Greenbaum Professor, Associate Dean for Curriculum John Glenn College of Public Affairs

March 23, 2025

Dear Professor Greenbaum:

I write to express the College of Law's full support of the proposed new stand-alone certificate on "Cybersecurity Law, Policy, and Management" (CLPM). This interdisciplinary certificate meets an important need for training public, nonprofit, and private sector managers about the institutions that currently govern cybersecurity policy.

It is our understanding that coursework for this specialization will be offered by the Glenn College, the Department of Electrical and Computer Engineering, and the Moritz College of Law. Once approved, the College of Law will be responsible for offering LAW 7805: Data Privacy, Cyber Security Regulation and Compliance and LAW 7804: Law of Cyberspace. This coursework will also be used as a new specialization in the Glenn College's MPAL degree and as a new track in the new Cybersecurity and Digital Trust master's degree.

Please keep us informed of each step of the approval process. I look forward to our continued collaboration with the Glenn College on this and other curricular efforts.

Very truly yours,

Annefalph

Anne Ralph Associate Dean for Academic Affairs & Strategic Initiatives Morgan E. Shipman Professor in Law The Ohio State University Moritz College of Law ralph.52@osu.edu /614-247-4797



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, Office of Academic Affairs
- From: Rosie Quinzon-Bonello, Assistant Dean for Curriculum and Assessment
- Date: April 18, 2025

Re: Revision to the Master of Public Administration and Leadership Degree

The College of Engineering supports the proposal submitted by the John Glen College of Public Affairs to establish a Cybersecurity Specialization in the Master of Public Administration and Leadership Degree.

Yours sincerely,

Resario Quijn - Bonello

Rosie Quinzon-Bonello

From:	Armstrong, Julia		
То:	Quinzon-Bonello, Rosario; Greenbaum, Rob		
Cc:	LIN, Zhiqiang		
Subject:	RE: Correction - RE: cybersecurity degree		
Date:	Thursday, April 10, 2025 11:17:44 AM		
Attachments:	image001.png		

Hello Rosie –

ICDT Supports the new the Embedded Graduate Certificate in Cybersecurity Law, Policy, and Management (CLPM). In addition, we also support he addition of the new specialization to the MPAL degree through the College of Engineering.

In the near future, I hope we will also be proposing a revision to the MCDT degree to include options in Cybersecurity Law, Policy, and Management for the students in that program.

Best,

Julia

Julia Armstrong, PMP

Managing Director, Institute for Cybersecurity and Digital Trust College of Engineering, The Ohio State University 599 Dreese Labs, 2015 Neil Ave., Columbus, OH 43210 614-688-1909 Office armstrong.798@osu.edu icdt.osu.edu

From: Quinzon-Bonello, Rosario <quinzon-bonello.1@osu.edu>
Sent: Thursday, April 10, 2025 9:18 AM
To: Armstrong, Julia <armstrong.798@osu.edu>; Greenbaum, Rob <greenbaum.3@osu.edu>
Subject: Correction - RE: cybersecurity degree

I got ECE mixed up with another proposal they are a part of. I still need to hear from both ECE and CSE regarding the cross-listed course.

Julia –

I have heard from ECE, just waiting for CSE. If I can have a brief statement that ICDT supports the proposal, that would be great. Email is fine.

Rosie

From: Armstrong, Julia <<u>armstrong.798@osu.edu</u>> Sent: Wednesday, April 9, 2025 6:07 PM To: Greenbaum, Rob <<u>greenbaum.3@osu.edu</u>>; Quinzon-Bonello, Rosario <<u>quinzon-bonello.1@osu.edu</u>> Subject: RE: cybersecurity degree

Hi Rob –

Yes, I can confirm that the intro class is offered by the ECE department each AU and SP (and is a large course! I believe between 75-90 enrolled each term?)

I've lost track of some of the emails. Is there anything you need from me/ICDT to confirm support? Julia

Julia Armstrong, PMP

Managing Director, Institute for Cybersecurity and Digital Trust College of Engineering, The Ohio State University 599 Dreese Labs, 2015 Neil Ave., Columbus, OH 43210 614-688-1909 Office armstrong.798@osu.edu icdt.osu.edu

From: Greenbaum, Rob <greenbaum.3@osu.edu>
Sent: Wednesday, April 9, 2025 4:39 PM
To: Quinzon-Bonello, Rosario <quinzon-bonello.1@osu.edu>
Cc: Armstrong, Julia <armstrong.798@osu.edu>
Subject: RE: cybersecurity degree

Hi Rosie,

Yes - that sounds great - thanks for your help!

Do you know if the plan is still for that Intro to Cybersecurity class to be offered each Autumn and Spring?

Rob

0

THE OHIO STATE UNIVERSITY

Robert T. Greenbaum Associate Vice Provost for Academic Programs Office of Academic Affairs Professor, Associate Dean for Curriculum John Glenn College of Public Affairs 350E Page Hall, 1810 College Road, Columbus, OH 43210 614-292-9578 Office / 614-292-2548 Fax https://glenn.osu.edu/rob-greenbaum Pronouns: he/him/his

From: Quinzon-Bonello, Rosario <quinzon-bonello.1@osu.edu>
Sent: Wednesday, April 9, 2025 3:17 PM
To: Greenbaum, Rob <greenbaum.3@osu.edu>
Cc: Armstrong, Julia <armstrong.798@osu.edu>
Subject: RE: cybersecurity degree

Hi Rob,

I talked to Dave about this today.

I have just copied you on an email I send to ECE and CSE curriculum reps.

Dave has requested that once I receive concurrence from ICDT and the two departments, I will write up a memo indicating college support and send it to you.

Does that work for you?

Thanks,

Rosie

THE OHIO STATE UNIVERSITY

Rosario (Rosie) Quinzon-Bonello, M.Ed. Assistant Dean for Curriculum and Assessment College of Engineering 122 Hitchcock Hall, 2070 Neil Ave. Columbus, OH 43210 quinzon-bonello.1@osu.edu engineering.osu.edu

From: Greenbaum, Rob <greenbaum.3@osu.edu>
Sent: Wednesday, April 9, 2025 12:58 PM
To: Quinzon-Bonello, Rosario <quinzon-bonello.1@osu.edu>
Cc: Ralph, Anne <ralph.52@osu.edu>
Subject: RE: cybersecurity degree

Hi Rosie,

I'm just following up regarding whether there is something more I should do to get our proposals to the two chairs for concurrence so we can hit Spring deadlines for curricular review (I think the Grad School/CAA curriculum committee meets soon).

I've attached a newer version of the MPAL proposal that combined the two documents. We plan to submit that simultaneously with the certificate proposal, which is a more complete proposal. I've attached that again and revised my letter at the front now reflect that we are submitting both together.

Thanks!

Rob

THE OHIO STATE UNIVERSITY

Robert T. Greenbaum Associate Vice Provost for Academic Programs Office of Academic Affairs Professor, Associate Dean for Curriculum John Glenn College of Public Affairs 350E Page Hall, 1810 College Road, Columbus, OH 43210 614-292-9578 Office / 614-292-2548 Fax

https://glenn.osu.edu/rob-greenbaum Pronouns: he/him/his

From: Tomasko, David <<u>tomasko.1@osu.edu</u>>
Sent: Friday, April 4, 2025 8:16 AM
To: Armstrong, Julia <<u>armstrong.798@osu.edu</u>>; Greenbaum, Rob <<u>greenbaum.3@osu.edu</u>>
Cc: Ralph, Anne <<u>ralph.52@osu.edu</u>>; Quinzon-Bonello, Rosario <<u>quinzon-bonello.1@osu.edu</u>>
Subject: Re: cybersecurity degree

Sorry I haven't been able to keep up with this.

Do the grad studies chairs in ECE and CSE know about the use of the course in this certifiate? If not, we should at least inform them and give them a change to review the proposal. I'd like to have buy in from ICDT (assume its there) and these two programs to put in a concurrence letter.

Julia - I don't know which meeting on monday you are referring to. Sorry. There are no committee meetings on my calendar at the moment.

David

David L. Tomasko Associate Dean for Academic Programs & Student Services Professor of Chemical & Biomolecular Engineering The Ohio State University If you have a zoom meeting scheduled with me: <u>https://osu.zoom.us/my/davidtomasko</u>

Executive Assistant: Winnie Sampson sampson.38@osu.edu 614-688-4602

If one accepts that without deeply understanding and being a part of society then one cannot develop meaningful solutions to the problems it presents, then current demographic trends in engineering are an actual threat to the profession.

From: Armstrong, Julia <armstrong.798@osu.edu>
Sent: Thursday, April 3, 2025 5:37 PM
To: Greenbaum, Rob <greenbaum.3@osu.edu>; Tomasko, David <tomasko.1@osu.edu>
Cc: Ralph, Anne <ralph.52@osu.edu>
Subject: RE: cybersecurity degree

Thank you Rob.

David - can you confirm this is on Monday's agenda?

(Also, I haven't heard about the time. Does that mean those who are proposing do not need to be there? In addition to this, there are also two new cybersec courses in the queue)

Cheers, Julia

Julia Armstrong, PMP

Managing Director, Institute for Cybersecurity and Digital Trust College of Engineering, The Ohio State University 599 Dreese Labs, 2015 Neil Ave., Columbus, OH 43210 614-688-1909 Office armstrong.798@osu.edu icdt.osu.edu

From: Greenbaum, Rob <greenbaum.3@osu.edu>
Sent: Wednesday, April 2, 2025 11:49 AM

To: Armstrong, Julia <<u>armstrong.798@osu.edu</u>>; Tomasko, David <<u>tomasko.1@osu.edu</u>>
Cc: Ralph, Anne <<u>ralph.52@osu.edu</u>>
Subject: RE: cybersecurity degree

Hi David,

Attached is the most recent version of the collaborative graduate certificate proposal. I'd love to include a letter from you similar to Anne's letter on page 3. Other than your letter, and the Registrar Sheet, I think it's ready to go.

We're also planning to send up an additional Cybersecurity Law, Policy, and Management specialization in our MPAL degree, with the ECE 5561/CSE 5471 intro course as the required course plus three additional courses from Moritz and Glenn, as long as you are okay with our including the Intro class as part of the program.

Thanks,

Rob

THE OHIO STATE UNIVERSITY

Robert T. Greenbaum Associate Vice Provost for Academic Programs Office of Academic Affairs Professor, Associate Dean for Curriculum John Glenn College of Public Affairs 350E Page Hall, 1810 College Road, Columbus, OH 43210 614-292-9578 Office / 614-292-2548 Fax

https://glenn.osu.edu/rob-greenbaum Pronouns: he/him/his

From: Armstrong, Julia <armstrong.798@osu.edu>
Sent: Monday, March 31, 2025 9:14 PM
To: Greenbaum, Rob <greenbaum.3@osu.edu>; Tomasko, David <tomasko.1@osu.edu>
Cc: Ralph, Anne <ralph.52@osu.edu>
Subject: RE: cybersecurity degree

David –

Should we set up a time for us all to discuss? Or is it possible to use this document to get on the upcoming CCAA agenda? (and we can discuss in the meantime)

I'd like to see this happen, though I still have some questions about how to best frame the write up.

Julia

Julia Armstrong, PMP

Managing Director, Institute for Cybersecurity and Digital Trust College of Engineering, The Ohio State University 599 Dreese Labs, 2015 Neil Ave., Columbus, OH 43210 614-688-1909 Office armstrong.798@osu.edu icdt.osu.edu

From: Greenbaum, Rob <greenbaum.3@osu.edu>
Sent: Friday, March 28, 2025 12:02 PM
To: Armstrong, Julia <armstrong.798@osu.edu>; Tomasko, David <tomasko.1@osu.edu>
Cc: Ralph, Anne <ralph.52@osu.edu>
Subject: RE: cybersecurity degree

Hi Julia and David,

Please find attached a brief proposal for the new track.

Regarding a. below, we also advocate for providing the students the option to add a third transciptable track to the degree. Each track is only 6 credit hours, and students currently have 9 hours of electives, so students could easily fit in three tracks and still have an elective.

Please let us know if you need anything else from us to consider the proposal.

In terms of after your committee approves this, I'm still trying to get clarity from the Graduate School regarding next steps (we are also trying to add a cybersecurity specialization to our MPAL degree). Maria Miriti's latest guidance was as follows:

The most important information to be communicated is the rationale for the specialization, the requirements, impacts on students and any administrative changes. There is a 4 week lead time for endorsement, but you should be ready to offer this come fall no matter what. Our next meeting is April 18 and then again at the end of May.

Also, David – would you be willing to provide us a letter supporting our proposed

Graduate Certificate in Cybersecurity, Law, Policy, and Management and MPAL specialization in Cybersecurity Law, Policy, and Management? Both require

ECE 5661/CSE 5471 - Introduction to Cybersecurity

Thanks much!

Rob



THE OHIO STATE UNIVERSITY

Robert T. Greenbaum Associate Vice Provost for Academic Programs Office of Academic Affairs Professor, Associate Dean for Curriculum John Glenn College of Public Affairs 350E Page Hall, 1810 College Road, Columbus, OH 43210 614-292-9578 Office / 614-292-2548 Fax

https://glenn.osu.edu/rob-greenbaum Pronouns: he/him/his

From: Armstrong, Julia <armstrong.798@osu.edu>
Sent: Friday, March 14, 2025 10:52 AM
To: Greenbaum, Rob <greenbaum.3@osu.edu>
Cc: Tomasko, David <tomasko.1@osu.edu>
Subject: RE: cybersecurity degree

Hi Rob –

I was buried in other MCDT related work this month with the recent approvals. Now is definitely the time to propose your additions. I believe the College needs to have these by the end of the month. Paperwork includes 3 items:

- 1. a short document on how the MCDT curricular plan would adjust to allow students to choose 2 of the 3 tracks. This may or may not be met with resistance.
- 2. A short document requesting the addition of elective courses should be smooth sailing.
- 3. A document that lists each course short description (and I think they'll also want a course syllabus for each)

I'm cc'ing David Tomasko to help me work through this. I would love to see it happen, but need a little guidance on how we can do this through the CCAA.

Julia

PS Thank you for that program listing for Ohio. No, I had not seen! That's quite helpful.

Julia Armstrong, PMP

Managing Director, Institute for Cybersecurity and Digital Trust College of Engineering, The Ohio State University 599 Dreese Labs, 2015 Neil Ave., Columbus, OH 43210 614-688-1909 Office armstrong.798@osu.edu icdt.osu.edu

From: Greenbaum, Rob <greenbaum.3@osu.edu>
Sent: Monday, March 3, 2025 9:54 AM
To: Armstrong, Julia <armstrong.798@osu.edu>
Subject: cybersecurity degree

Hi Julia,

Congratulations on the new degree finally being approved!

We're working to get our certificate in the approval pipeline very soon. Say, do you know what we need to do to propose our track to be added to the degree? Do you have any feedback on what we are proposing? Our proposed additions are in red in the attached document.

Also, in case it is helpful for your work to create an undergraduate degree, a colleague shared the attached list of programs in Ohio. I'm not sure who created it - maybe it even came from you?

Take care,

Rob

The Ohio State University

Robert T. Greenbaum Associate Vice Provost for Academic Programs Office of Academic Affairs Professor, Associate Dean for Curriculum John Glenn College of Public Affairs 350E Page Hall, 1810 College Road, Columbus, OH 43210 614-292-9578 Office / 614-292-2548 Fax https://glenn.osu.edu/rob-greenbaum Pronouns: he/him/his

From:	Williamson, Donald			
То:	Greenbaum, Rob; Quinzon-Bonello, Rosario			
Cc:	<u>Qin, Fenq</u>			
Subject:	Re: cybersecurity degree			
Date:	Friday, April 18, 2025 7:34:26 AM			
Attachments:	image001.png			
	image002.png			
	image003.png			

Hi everyone,

The CSE curriculum committee is fine with inclusion of this course within the proposed program.

Best,

Donald S. Williamson Associate Professor Director, <u>The ASPIRE Group</u> Affiliated faculty, Translational Data Analytics Institute Computer Science and Engineering 493 Dreese Labs, 2015 Neil Ave, Columbus, OH 43210 williamson.413@osu.edu



THE OHIO STATE UNIVERSITY COLLEGE OF ENGINEERING

From: Greenbaum, Rob <greenbaum.3@osu.edu>
Date: Wednesday, April 16, 2025 at 1:39 PM
To: Williamson, Donald <williamson.413@osu.edu>, Qin, Feng <qin.34@osu.edu>
Cc: Quinzon-Bonello, Rosario <quinzon-bonello.1@osu.edu>
Subject: RE: cybersecurity degree

Thanks much for this update.

The Graduate School indicated that we should be okay in terms of timing for their last meeting of the year if we can submit the proposals before Friday, so that timing works well.

Rob



THE OHIO STATE UNIVERSITY

Robert T. Greenbaum Associate Vice Provost for Academic Programs Office of Academic Affairs Professor, Associate Dean for Curriculum John Glenn College of Public Affairs 350E Page Hall, 1810 College Road, Columbus, OH 43210 614-292-9578 Office / 614-292-2548 Fax

https://glenn.osu.edu/rob-greenbaum Pronouns: he/him/his

From: Williamson, Donald <williamson.413@osu.edu>
Sent: Wednesday, April 16, 2025 1:09 PM
To: Qin, Feng <qin.34@osu.edu>
Cc: Quinzon-Bonello, Rosario <quinzon-bonello.1@osu.edu>; Greenbaum, Rob
<greenbaum.3@osu.edu>
Subject: Re: cybersecurity degree

Hi Feng and Rob,

I'm hoping to finalize a response for this within the next day or so. I shared with CSE's curriculum committee earlier, and I reached out to them for any feedback. I'll let you know if there are any questions or comments to share.

Best,

Donald S. Williamson Associate Professor Director, <u>The ASPIRE Group</u> Affiliated faculty, Translational Data Analytics Institute Computer Science and Engineering 493 Dreese Labs, 2015 Neil Ave, Columbus, OH 43210 williamson.413@osu.edu



THE OHIO STATE UNIVERSITY COLLEGE OF ENGINEERING

From: Qin, Feng <<u>qin.34@osu.edu</u>>
Date: Wednesday, April 16, 2025 at 11:34 AM
To: Williamson, Donald <<u>williamson.413@osu.edu</u>>
Cc: Quinzon-Bonello, Rosario <<u>quinzon-bonello.1@osu.edu</u>>
Subject: FW: cybersecurity degree

Hi Donald (cc'd Rosie),

You may have received this already. Any comments?

Best, Feng From: Quinzon-Bonello, Rosario <<u>quinzon-bonello.1@osu.edu</u>> Date: Wednesday, April 16, 2025 at 11:13 AM To: Qin, Feng <<u>qin.34@osu.edu</u>> Subject: FW: cybersecurity degree

Hello Feng,

I think I maybe I should have the email below to you which concerns cross-listed courses ECE 5561 / CSE 5471 *Introduction to Cybersecurity,*

I have heard back from ECE granting concurrence to include ECE 5561 in the attached proposal submitted by the Glen College of Public Affairs.

We are just waiting on CSE's concurrence. Once I receive that, I can send off a memo of support from the college.

Thanks, Rosie

From: Quinzon-Bonello, Rosario
Sent: Wednesday, April 9, 2025 3:14 PM
To: Ekici, Eylem <<u>ekici.2@osu.edu</u>>; Williamson, Donald <<u>williamson.413@osu.edu</u>>
Cc: Greenbaum, Rob <<u>greenbaum.3@osu.edu</u>>; Armstrong, Julia <<u>armstrong.798@osu.edu</u>>
Subject: FW: cybersecurity degree

Hello Eylem and Donald,

Attached is a proposal submitted by the John Glenn College of Public Affairs to establish a Type 3a Stand Alone and 3b Embedded Graduate Certificate in Cybersecurity Law, Policy, and Management (CLPM).

The curriculum includes the following cross-listed course

ECE 5561 / CSE 5471 Introduction to Cybersecurity

Please provide feedback / concurrence for the inclusion of this course in the proposal by Friday, April 18.

Thank you,

Rosie

Hi Rosie,

I am fine with the inclusion of this course in the proposed certificate program.

Eylem

--Dr. Eylem Ekici

ProfessorDept. of Electrical and Computer Eng.Phone: (614) 292-0495The Ohio State UniversityFax: (614) 292-7596

http://u.osu.edu/ekici

E-mail: <u>ekici.2@osu.edu</u>

From: Quinzon-Bonello, Rosario <quinzon-bonello.1@osu.edu>
Date: Wednesday, April 9, 2025 at 3:13 PM
To: Ekici, Eylem <ekici.2@osu.edu>, Williamson, Donald <williamson.413@osu.edu>
Cc: Greenbaum, Rob <greenbaum.3@osu.edu>, Armstrong, Julia
<armstrong.798@osu.edu>
Subject: FW: cybersecurity degree

Hello Eylem and Donald,

Attached is a proposal submitted by the John Glenn College of Public Affairs to establish a Type 3a Stand Alone and 3b Embedded Graduate Certificate in Cybersecurity Law, Policy, and Management (CLPM).

The curriculum includes the following cross-listed course

ECE 5561 / CSE 5471 Introduction to Cybersecurity

Please provide feedback / concurrence for the inclusion of this course in the proposal by Friday, April 18.

Thank you,

Rosie

Proposal for a Type 3a and 3b Certificate in Cybersecurity Law, Policy, and Management

Submitted by John Glenn College of Public Affairs Moritz College of Law

To Be Approved by Faculty, John Glenn College of Public Affairs on 5/10/2024 Graduate Studies Committee Approved on 01/12/2024

Program Overview

The John Glenn College and the Moritz College of Law propose a new stand-alone and embedded certificate on "Cybersecurity Law, Policy, and Management" (CLPM). The certificate is a 15-credit hour program.

The certificate is interdisciplinary. The introductory course on cybersecurity technical, social, and management issues would be offered by the Department of Electrical and Computer Engineering in the College of Engineering (COE). Students are then required to take four core courses, with the option of taking one elective to substitute for one core course. With careful planning, it is envisioned that students could complete the certificate in three semesters (one calendar year).

The design of this proposed stand-alone certificate took into consideration the new collaborative College of Engineering Masters in Cybersecurity and Digital Trust degree. Therefore, the courses offered by the Glenn College and Moritz College will assume an introductory knowledge of the technical fundamentals of data, software, components, networks provided by the COE introductory course on cybersecurity.

Rationale

The CLPM certificate will fill help fill an important gap in addressing the need to train public, nonprofit, and private sector managers about the institutions that currently govern cybersecurity policy. Cybersecurity is a public good and must be collectively governed by the public, nonprofit, and private sectors. Federal and state law and policy provide the foundational formal rules for these 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, policy makers, 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. As the legal profession continues to specialize, the courses in the CLPM certificate could provide the opportunity for newly graduated attorneys to accelerate their careers.

Certificate Objectives

The CLPM is designed to meet the needs of those who are: 1) professional managers already working in the field who need additional specialized training in cybersecurity; 2) managers who are contemplating a career shift into this growing professional field; 3) technologists who want to develop increased competence in implementing technical solutions by taking complementary training in policy and management; 4) qualified graduates of undergraduate programs who have an interest in starting a career in cybersecurity; and 5) attorneys who see an opportunity in specializing in cybersecurity law and management. Professionals completing this certificate will have a:

- 1. A foundational understanding of the kinds of cybersecurity threats that exist through an introductory course on cybersecurity;
- 2. A strong mental model of organizations as systems of "information flows" that will enable professionals to wholistically think about reducing the risk of cybersecurity threats as against other competing information processing needs of the organization through a course on Data Governance;
- 3. A broad understanding of the law of cyberspace, especially the cutting-edge issues that arise from technological change with an emphasis on the Law of Privacy;
- 4. A broad understanding of cybersecurity policy at the federal and state (Ohio) level;
- 5. A "cognitive map" of the important organizations in managing cybersecurity including their roles and their interrelationships;
- 6. A decision-making framework to support policymakers and managers in a complex legal, policy, engineering, and managerial environment where each domain has its own norms and ways of thinking. The integrated framework provides the foundation to better understand the cybersecurity management tools that exist and how to use them.

Market Assessment

A market assessment for the CLPM indicates that there is demand for graduates of this program. To address that demand, the CLPM could occupy a unique educational niche among State of Ohio online graduate programs. Two market assessments were completed each using a different source of data. The first assessment was conducted by the Glenn and Moritz Colleges using data supplied by "Cyberseek". The second assessment was conducted by OSO and is included as an Appendix. (Forthcoming).

Market Demand

Cyberattacks and cybersecurity are a growing problem. The F.B.I.'s Internet Cybercrime Complaint Center (IC3) reported that in 2022 it received "800,944 complaints, which is a 5 percent decrease from 2021. However, the potential total loss has grown from \$6.9 billion in 2021 to more than \$10.2 billion in 2022."¹ See Figure 1. The actual costs are probably far higher since it is well-known that there is a significant underreporting of crimes.² Clearly, there is much work to be done and a growing need for graduates to fill the shortage of shortage of professionals to respond to these threats.



Figure 1: Growth in Cybersecurity Complaints and Costs

Source: https://www.ic3.gov

"CyberSeek" is a joint effort of the National Institute of Standards and Technology

¹ U.S. Federal Bureau of Investigation, Internet Crime Complaint Center,

[&]quot;2022 Internet Crime Report"

²https://www.researchgate.net/publication/368293083_Measuring_Cybercrime_and_Cyberdeviance_in_S urveys

(NIST) and two workforce development companies to supply information on cybersecurity employment and training.³ This proposal conducted a market assessment using the Cyberseek website to determine both the growth in cybersecurity jobs and employment as well as the online graduate programs now offered in Ohio.

Since 2010, there has been an 82% increase in the number of cybersecurity openings and a 60% increase in the size of the workforce for the State of Ohio. (Total Ohio Job Openings in 2023 are 166 and Total Ohio Employment is 267). (Total National Job Openings in are 572,392 and Total National Employment is 1,178,662). See Figure 2.

Figure 2: Growth in National and Ohio Cybersecurity Workforce



Source: https://www.cyberseek.org/heatmap.html

Market supply

The Cyberseek website provided information on cybersecurity programs within Ohio. A search was conducted on the set of all online graduate programs in Ohio. The results indicated that the Glenn College / Moritz Certificate in Cybersecurity Law, Policy, and Management would be the only interdisciplinary program (Law / Policy and Management) offered in the State of Ohio. See Table 1.

³ https://www.cyberseek.org/index.html#partners

University	Program	Compare	Credits	Duration
Cleveland	Online	Focus is on	30 credits	
State	Masters of	Law		
University	Legal Studies			
College of	in			
Law	Cybersecurity			
	and Data			
	Privacy -			
	Synchronous			
	and			
	Asynchronous			
Findlay	Master's	No law policy,	12 2 core	2 years
University	Online and	three	courses, 2	
	On-campus	management	electives	
		courses		
University of	Certificate (or	Engineering	12 credits, 4	Full-time or
Cincinnati	as part of		required	part-time
	Masters in			option
	<u>Information</u>			
	Technology)			
Wright State	Master of	Technical but	30 credits	
University	Science in	does require		
	<u>Cybersecurity</u>	introduction to		
		information		
		security		
		(similar to		
		ECE 5651) and		
		offers elective		
		Legal Aspects		
		of		
		Cybersecurity		

Table 1: Online Graduate Cybersecurity Programs in Ohio

Source: Identification of Programs taken from Cyberseek website:

<u>https://www.cyberseek.org/heatmap.html</u>. Program information on degree offered credit hours taken from scan of individual university program websites.

Curriculum

The CPLM is intentionally designed to fill a curricular gap and meet the needs of those who are: 1) professional managers already working in the field who need additional specialized training in cybersecurity; 2) managers who are contemplating a career shift into this growing professional field; and 3) technologists who want to develop increased competence in implementing technical solutions by taking complementary training in policy and management; 4) qualified graduates of undergraduate programs who have an interest in starting a career in cybersecurity; and 5) attorneys who see an opportunity in specializing in cybersecurity law and management.

The CLPM is a fifteen-credit certificate. All students are required to take the Introduction to Cybersecurity course offered by the College of Engineering. Students must then take four more courses. Three of those additional courses must be core courses. Students can take one elective course to substitute for a core course. See Table 2 below.

Table 2: CLPM Curricular Plan

Core Courses				
College of Engineering (3 credits)				
ECE 5561/CSE 5471 - Introduction to Cyl	ECE 5561/CSE 5471 - Introduction to Cybersecurity			
Introduction to cybersecurity. Technical fundamentals of data, software, component,				
network, and system security. Cybersecurity	from an organizational and societal			
viewpoint, including human factors.				
Glenn College Moritz College ⁴				
PUBAFRS 5510 – Cybersecurity Law,	LAW 7804 - Law of Cyberspace (3)			
Management, and Policy (3) (New				
Cybersecurity Course)	Allows students with varying backgrounds			
	to confront the cutting-edge legal issues			
Designing and managing a robust	that arise from technological change and			
cybersecurity architecture using law,	the Internet.			
policy, and management.				
PUBAFRS 5570 - Data & Information	LAW 7805 - Data Privacy, Cyber			
Governance (3) (New Cybersecurity	Security Regulation and Compliance (3)			
Course)	This course examines the legal, policy,			
	and operational management issues related			
Concepts and skills to manage	to data privacy and data protection.			
cybersecurity from a data governance				
perspective.				

Elective Courses			
PUBAFRS 5770 – Risk and Decision Analysis (3 credits)			
PUBAFRS 6050 - Managing Public Organizations (4 credits)			
PUBAFRS 6055 - Judgement in Managerial Decision-Making (2 credits)			
PUBAFRS 6530 – Negotiation (1 credits)			
PUBAFRS 7553 – Nonprofit Management and Governance (3 credits)			
PUBAFRS 7555 – Project Management (3 credits)			
PUBAFRS 7600 – Federal Policy and Management (3 credits)			

⁴ While the Moritz classes are 7000-level classes, these classes are open to students outside of the Moritz College and are generally more accessible to the layperson than required classes in the JD program.

Glenn College and Moritz College faculty or instructors with professional experience in a related field will teach the courses. Glenn College courses will be taught online asynchronously while Moritz College courses will be taught online synchronously. Recordings of the Moritz College classes will be made available for students who cannot attend during the scheduled class hours.

Assessment

Assessing whether the certificate is meeting the certificate objectives and accreditation requirements will be undertaken separately for each college given their differing accreditation requirements.

Moritz College of Law

The College requires students in the M.S.L. program to take two required courses, designed to help students gain a basic understanding of the legal system and achieve the program learning goals outlined below. The College examines student feedback from the student evaluation of instruction instrument used by the law school. Finally, the staff of the M.S.L. program seeks individual feedback from students to improve the programming and counseling provided to student each year. All this information is regularly used to monitor and improve the quality of the program.

The College's MSL program assessment plan includes the following outcomes and assessment methods:

- **Outcome 1: Basic understanding of the legal system.** Students in the Masters for the Study of Law program will gain a basic understanding of law, legal institutions, and legal culture, including essential substantive and procedural elements.
 - Students are required to demonstrate achievement of this outcome by successfully completing the Intro to the US Legal System, LAW-8525 (3 credits) and Legal Research and Writing, LAW-8550 (3 credits).
- Outcome 2: Legal Doctrine and Substantive Knowledge. Professionals working in and adjacent to law use specialized words and concepts. To work effectively in a field related to law, a professional must understand core legal concepts and specialized doctrine in the legal practice area. Legal "doctrine," moreover, encompasses more than the black-letter rules in a field; it includes the ambiguities and open issues within that field.
 - Students receive substantive knowledge and legal doctrine through the Intro to the US Legal System course. In addition, all MSL students must receive passing scores in the Legal Research and Writing course, which includes foundational instruction in legal writing, research, and analysis and substantial writing assignments. Students' achievement of this outcome are assessed in those courses.
 - The College evaluates the effectiveness of the program in part through the feedback students provide for each class with regard to the quality of the course and instructor and the critical thinking skills developed.

- Outcome 3: Ability to Use Law-Related Materials and Processes. Lawyers use specialized materials, including judicial opinions, statutes, regulations, contracts, etc. Professionals working in fields related to law will benefit by knowing how to find, interpret, and apply the materials relevant to their work. Similarly, lawyers participate in a large number of law-related processes. Professionals in allied fields should be familiar with the legal processes they will encounter in their areas of expertise.
 - Students develop these skills in, among other courses, Legal Research and Writing. In addition, all MSL students must receive passing scores in the Legal Research and Writing course, which includes foundational instruction in legal writing, research, and analysis and substantial writing assignments.
- Outcome 3: Critical Thinking and Problem-solving. Lawyers think critically about problems. Most lawyers use at least four types of critical thinking: (1) deductive reasoning, (2) cost-benefit analysis, (3) thinking by analogy, and (4) viewing problems from competing perspectives. Professionals in fields associated with law should recognize and be able to apply these thought processes to the problems that arise in their field.
 - Most courses in the MSL program cover these areas of critical thinking to varying degrees, but are highlighted in through the Intro to the US Legal System course and applied in the Legal Research and Writing course, and students' achievement of this outcome are assessed in those courses.
- **Outcome 4: Communication.** Legal work relies upon many communication methods that include both receiving information and imparting it. To work effectively in a field related to law, other professionals must communicate effectively with lawyers.
 - Most courses in the MSL program include assignments that require students to develop and demonstrate communication skills. These skills are most rigorously developed and assessed in the Legal Research and Writing course.

John Glenn College of Public Affairs

Upon completion of CLPM, students meet the following program leaning objectives at an *intermediate* level as they will be better prepared to

- Policy 3 Understand the legal foundations of policy and management in the public sector.
- Policy 8 Understand legal reasoning.
- Policy 9 Understand how the law can be used to achieve public goals.
- *Mgt 1 Manage and lead public organizations towards policy goals.*
- *Mgt* 5 *Engage in strategic planning for public organizations.*
- *Mgt* 8 *Manage innovation and change.*
- *Methods* 2 *Manage storage and retrieval of data.*
- *Methods 3 Understand the role of information technology in managing and leading an organization.*

Direct assessment: Students will be assessed through examinations, in-class, and out-of-

class exercises. Each assessment tool will be mapped to one or more of the above curricula learning goals. Instructors will assess whether students exceed/meet/do not meet. This will be performed annually and modifications to the curriculum will be made based on the results of these assessments.

Indirect assessment: The Glenn College will track the careers of the CLPM alumni. A post-program survey of students that investigates areas for improvement in the curriculum will also be conducted.

Eligibility

Admission to, performance in, and exit standards for the certificate are consistent with the Graduate School's standards for admission and progression. Admission requirements include a baccalaureate degree from an accredited institution with a minimum cumulative GPA of 3.0 (on a 4.0 scale or equivalent) for the last bachelor's or advanced degree earned. Personal statements require articulation of how the certificate is consistent with the applicant's professional and career goals. Students from international undergraduate institutions are recommended to score at least a 100 in the TOEFL iBT. Resumes and transcripts are required from all applicants.

A minimum cumulative GPA of 3.0 is required to receive a certificate, and only grades of A through C- may be counted toward the completion of the certificate program.

Administrative Arrangements for the Proposed Program

Marketing

As part of the agreement to develop online programs, OSO would market the CLPM with supplemental funding from the Glenn and Moritz Colleges. Typically, OSO works the departments and colleges to create a strategic marketing plan, which includes additional marketing efforts carried out the Glenn College.

Recruitment and admissions

Under the new online model, Ohio State Online will take the lead on recruitment and initial contact and questions about admissions for students enrolling in the CLPM. They will work closely with the Glenn College and the Moritz College. The Glenn College will be the primary unit to make admissions decisions.

Advising and student support

Advising and student support for students enrolling in the Glenn / Moritz Cybersecurity Certificate will be provided primarily by the Glenn College. OSO will provide more general student support as students progress through the certificate.

Career advising

The Glenn College currently provides instruction on how to use online job search searches. It also assists students in writing resumes and how to interview for a job. At the present time, however, there is no resident expertise on working in the cybersecurity field. There is an effort underway to determine career paths so that students in the CLPM can identify additional coursework at Ohio State for career paths. (The NICE framework supported by NIST identifies job descriptions and their respective competencies.)

Tuition and student fees

Students pay the typical Graduate School tuition and fees for an online program.

Planned Enrollment

The CLPM expects to enroll five to seven new students each semester, inclusive of students in the stand-alone certificate and embedded certificate (Glenn MPA, MPAL, and Moritz MSL students), with approximately twenty students enrolled in the program full-time.



Curriculum Proposal Checklist

Title of Prog	ram:							
Effective tern	n:		Col	lege:				
New/Establis	sh: Second	ary Major Eligible:	Aca	demic Un	it:			
Revise:	50% Revision:	Mark Up:	Pro	gram Con	itact:			
Terminate:	Susper	nd:	Certifi	cate Categ	gory*:			
Degree/Cred	ential:							
Program of S	Study :		Ti	tle:				
Code:								
Program Foc	us*:							
Credit hours	to degree/crede	ntial:	Is this	a change	e to the current	total?	Yes	No
Program offe	ered only online	Yes No	If yes, is	s there a si	igned MOU wi	th ODEE?	Yes	No
Campus(es) where offered: Columbus A			ATI	Lima	Mansfield	Marion	Newa	rk

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

Memorandum of Understanding

Between

Graduate Certificate (3a and 3b) in Cybersecurity Law, Policy, and Management The John Glenn College of Public Affairs [administrative lead] and The Moritz College of Law

The Ohio State University

And

Ohio State Online The Ohio State University

Purpose

The purpose of this Memorandum of Understanding (MOU) is to acknowledge that the **Graduate Certificate in Cybersecurity Law, Policy, and Management** has met or exceeded the modality substantive change threshold, making the program an online program or is a new online program for the university and will meet the requirements for an online program in partnership with Ohio State Online.

Term of MOU

This MOU will begin effective upon obtaining all necessary signatures and will remain in effect for the life of the program.

Services Provided for Program Launch

As an online program this program will receive Ohio State Online support, such as market research, student acquisition, ongoing student support, online program and course design and development, and state authorization and licensure research and disclosures (if applicable).

Based on pre-approval planning conversations, this program may leverage the following Ohio State Online services:

Online Enrollment Services: Generating and finding quality prospective students, selling prospective students on the program and Ohio State, helping re-enroll students each term to



help them reach graduation, and supporting the college to recognize steady-state revenue streams.

Online Instruction Services: Reviewing and recommending evidence-based online program curricular design to best meet and support the intended audience and enrollment goals; providing and encouraging online instructor professional learning opportunities; and partnering with instructors for initial course design, development, and ongoing course updates.

It is expected Ohio State Online and program relationship contacts below will remain in discussions as part of ongoing college check-ins to evolve services to achieve program goals.

Table of Program Relationship Contacts

Units	College / Department / Campus	Ohio State Online	
Organization Oversight	-Kent Barnett, Dean (Moritz) -Trevor Brown, Dean (Glenn)	Jason Lemon, Dean	
Administrative Oversight	 Anne Ralph, Associate Dean for Academic Affairs & Strategic Initiatives (Moritz) Rob Greenbaum, Associate Dean for Curriculum (Glenn) 	 Rob Griffiths, AVP, Online Learning and Innovation Brandi Bittner, AVP, Online Enrollment 	
Program Oversight	 Rob Greenbaum, Associate Dean for Curriculum (Glenn) Jim Landers, Graduate Studies Chair (Glenn) Chris Adams, Director of Student Services and Programs (Glenn) 	 Rob Griffiths, AVP, Online Learning and Innovation Brandi Bittner, AVP, Online Enrollment 	
Course Oversight	 Rob Greenbaum, Associate Dean for Curriculum (Glenn) Aaron Carpenter, Senior Instructional Designer (Glenn) 	John Muir, OSO program / course design innovation, assigned Instructional Designer	
Student Support Oversight	- Kate Hallihan, Assistant Dean of Students and Instruction	Assigned Reenrollment Specialist	


	(Glenn) - Lindsey Lee, Program Manager (Glenn) - Mindy Niehaus, Program Manager (Glenn)	
Marketing/Recruiting Oversight	 Erin Trueman, Director of Marketing and Communications (Glenn) Syndey Rubin, Recruitment and Engagement Specialist (Glenn) 	Assigned Marketing Manager and Recruiting lead
Fiscal Oversight	 Matt Yoder, CFO (Moritz) Kim Young, CAO/SFO (Glenn) 	AVP, OSO Financial Strategy and Analysis

Signatories

By signing this MOU, all groups agree to be active partners and to abide by this agreement:

DocuSigned by:	
Program Director James Richard Landers	Date: 11/15/2024
Department Chair Clustopher John Adams	Date: 11/18/2024
College Fiscal Officer Limbury lune young	Date: 11/18/2024
Curricular Associate Dean Robert Greenbarn	Date: 11/18/2024
Dean Trivor Lawring Brown 6DC90E2317E24C9 DocuSigned by:	Date: 11/18/2024
Vice Provost and Dean of Online Learning Jason Edward Lumon	Date: 11/18/2024

Online Program Attributes

Program Working Title: Graduate Certificate in Cybersecurity Law, Policy, and Management

Anticipated CAA approval date for ONL modality: **AU24** Anticipated ODHE approval date for ONL modality: **n/a**

Program level:

Associate Undergraduate	🛛 Graduate 🗌] Professional
-------------------------	--------------	----------------

Approval type:

🛛 New program 🗌] Change of deliver	y \boxtimes Certificate	Stackable] Other
-----------------	---------------------	---------------------------	-----------	---------

If applicable, will the program continue to offer an on-ground version? Note, notification to CAA and Ohio State Online will be necessary if an approved program modality is no longer offered.

🗌 Yes 🔄 No

Percentage of courses offered online for this program?

🖂 100%	80-99%
--------	--------

If other, please explain:

Anticipated term for first cohort: AU25

Note, marketing and recruitment will begin approximately 6 months prior to first enrollment term.

Will this program have a different fee structure from what would normally be assessed to similar students at the university?

Note, submissions are due in December for Senate Fiscal review—<u>Financial Planning</u> and Analysis and Student Fee Review Committee review is necessary for differentiated <u>tuition</u>. Once Senate Fiscal Committee recommendations are finalized, the request goes to the President and Provost for review and then for the official Board of Trustees approval.

🗌 Yes

🖂 No

If yes, please explain justification:



THE OHIO STATE UNIVERSITY

Total credit hours for program: 15

Does this program have mandatory onsite training components? (e.g., practicum, residency, or internship)

🗌 Yes 🛛 🖾 No

If yes, please explain:

Does this program have any non-mandatory onsite training components? (e.g., orientation)

🗌 Yes 🛛 🖾 No

If yes, please explain:



Program Courses

The online program course delivery strategy at launch is outlined in the table below.

Note: the information in the first row of the table is included only to provide an example of how the information should be formatted.

Course Code and Name	Current Delivery Mode(s)* (how course has been offered previously: in person, hybrid, distance learning, N/A - new course)	Core or Elective	Asynchronous or Synchronous or Both	First Term and Session (if applicable) this Course will be Offered as part of this Online Program	Other terms and sessions (if applicable) this course be offered (None, AU25, SP25, SU25)
ECE 5661/CSE 5471		Core		AU25	Each AU & SP
PUBAFRS 5510	N/A – new course	Core	Asynchronous	SP25	Each SP
PUBAFRS 5570	N/A – new course	Core	Asynchronous	AU25	Each AU
LAW 7804	DL, P	Core	Asynchronous	SU25	Each SU (DL 7 weeks), Each SP (P)
LAW 7805	DL, P	Core	Asynchronous	AU25	Each AU (DL 7 weeks), Each AU (P)
PUBAFRS 5770	DL	Elective	Asynchronous	AU 25	Likely each AU
PUBAFRS 6050	DL, Hybrid	Elective	Asynchronous	AU25	Each AU, SP, SU
PUBAFRS 6055	DL	Elective	Asynchronous	SP26	Each SP, SU
PUBAFRS 6530	DL, P	Elective	Asynchronous	AU25	Each AU, SP, SU
PUBAFRS 7553	DL, HY	Elective		AU25	Each AU, SP



PUBAFRS 7555	DL, P	Elective	Asynchronous	AU25	Each AU (P), SP, SU
PUBAFRS 7600	DL, P (in DC)	Elective	Asynchronous	SP26	Each SP

State Authorization / Disclosure

Ohio State Online will support necessary steps for approvals and notifications, and the program will abide by state laws and disclosure requirements, for items selected yes.

	Yes/No
Enroll students located outside Ohio?	Yes
Does this program potentially lead to a professional license or certification in any state?	No
Conduct on-ground supervised field experiences such as clinicals, practicums, student teaching or internships?	No



Certificate Of Completion

Envelope Id: B0464B10556F42FFAB0FBF833CA8F8B0 Subject: Complete with Docusign: MOU - Cybersecurity Law Policy and Management OSO MOU Source Envelope: Document Pages: 7 Signatures: 6 Certificate Pages: 7 Initials: 0

AutoNav: Enabled Envelopeld Stamping: Enabled Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Record Tracking

Status: Original 11/13/2024 11:05:13 AM

Signer Events

James Richard Landers landers.1@osu.edu The Ohio State University

Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure: Not Offered via DocuSign

Christopher John Adams

adams.615@osu.edu

Director of Student Services

The Ohio State University

Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure: Not Offered via DocuSign

Kimberly Anne Young young.1807@osu.edu

Chief Administrative Officer

The Ohio State University Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure: Not Offered via DocuSign

Robert Greenbaum greenbaum.3@osu.edu Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure: Accepted: 7/19/2023 10:25:10 AM ID: 88c5af2e-9012-482c-897d-78a03a4a1010 Company Name: The Ohio State University

Holder: Jonathan Mark Rucker rucker.78@osu.edu

Signature

DocuSigned by: James Richard Landers 47747559574F4B7...

Signature Adoption: Pre-selected Style Using IP Address: 65.60.165.139

Christopher John Adams

Signature Adoption: Pre-selected Style Using IP Address: 128.146.244.172

Status: Completed

Envelope Originator: Jonathan Mark Rucker 1050 Carmack Rd Columbus, OH 43210 rucker.78@osu.edu IP Address: 128.146.238.57

Location: DocuSign

Timestamp

Sent: 11/15/2024 9:22:37 AM Viewed: 11/15/2024 2:42:34 PM Signed: 11/15/2024 2:42:46 PM

Sent: 11/15/2024 2:42:48 PM Viewed: 11/18/2024 9:46:01 AM Signed: 11/18/2024 10:26:22 AM

Sent: 11/18/2024 10:26:25 AM Viewed: 11/18/2024 10:27:45 AM Signed: 11/18/2024 10:30:54 AM

Sent: 11/18/2024 10:30:56 AM Viewed: 11/18/2024 10:39:18 AM Signed: 11/18/2024 10:39:54 AM

kimberly anne young 4B294819E20405

Signature Adoption: Pre-selected Style Using IP Address: 76.224.1.228

DocuSigned by: Robert Greenbaum FBA4EEA355734D5...

Signature Adoption: Pre-selected Style Using IP Address: 140.254.174.158



Signer Events	Signature	Timestamp
	DocuSigned by:	Sent: 11/18/2024 10:39:56 AM
brown 2296@osu edu	Trevor Lawrence Brown	Viewed: 11/18/2024 10:39:50 AM
Dean	6DC90E2317E24C9	Signed: 11/18/2024 10:41:04 AM
The Ohio State University		e.g. ear + , , e, 202 + , er + , e + , in
Security Level: Email, Account Authentication	Signature Adoption: Pre-selected Style	
(None)	Using IP Address: 184.57.9.197	
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Jason Edward Lemon	DocuSigned by:	Sent: 11/18/2024 10:41:07 AM
lemon.297@osu.edu	Jason Edward Lemon	Viewed: 11/18/2024 4:58:14 PM
Security Level: Email, Account Authentication	9C19184E034F41C	Signed: 11/18/2024 4:58:42 PM
(None)		ů.
	Signature Adoption: Pre-selected Style	
	Using IP Address: 23.245.222.250	
Electronic Decord and Signature Disclosure.	Signed using mobile	
Not Offered via DocuSign		
In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Carbon Copy Events Robert Peter Griffiths	Status	Timestamp Sent: 11/18/2024 4:58:44 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu	Status COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University	Status COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None)	Status COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign	Status COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner	Status COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu	Status COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu Security Level: Email, Account Authentication (None)	Status COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign	Status COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Jonathan Mark Rucker	Status COPIED COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:47 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Jonathan Mark Rucker rucker.78@osu.edu	Status COPIED COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:45 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Jonathan Mark Rucker rucker.78@osu.edu Security Level: Email, Account Authentication (None)	Status COPIED COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:47 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Jonathan Mark Rucker rucker.78@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Electronic Record and Signature Disclosure: Not Offered via DocuSign	Status COPIED COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:47 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Jonathan Mark Rucker rucker.78@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Jonathan Mark Rucker rucker.78@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Electronic Record and Signature Disclosure: Not Offered via DocuSign Electronic Record and Signature Disclosure: Not Offered via DocuSign Electronic Record and Signature Disclosure: Not Offered via DocuSign	Status COPIED COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:47 PM Sent: 11/18/2024 4:58:47 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Jonathan Mark Rucker rucker.78@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Jonathan Mark Rucker rucker.78@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Electronic Record and Signature Disclosure: Not Offered via DocuSign Erin R McLaughlin mclaughlin.556@osu.edu	Status COPIED COPIED COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:47 PM Sent: 11/18/2024 4:58:47 PM
Carbon Copy Events Robert Peter Griffiths griffiths.44@osu.edu The Ohio State University Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Brandi N Bittner bittner.102@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Jonathan Mark Rucker rucker.78@osu.edu Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign Electronic Record and Signature Disclosure: Not Offered via DocuSign Electronic Record and Signature Disclosure: Not Offered via DocuSign Erin R McLaughlin mclaughlin.556@osu.edu Security Level: Email, Account Authentication (None)	Status COPIED COPIED COPIED	Timestamp Sent: 11/18/2024 4:58:44 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:45 PM Sent: 11/18/2024 4:58:47 PM Sent: 11/18/2024 4:58:47 PM Sent: 11/18/2024 4:58:47 PM

Carbon Copy Events	Status	Timestamp
John Muir	CODIED	Sent: 11/18/2024 4:58:49 PM
muir.25@osu.edu	COPIED	
The Ohio State University		
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Meri Ellen Lynott	COPIED	Sent: 11/18/2024 4:58:50 PM
lynott.6@osu.edu	COFILD	
The Ohio State University		
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Jennifer L Simmons	COPIED	Sent: 11/18/2024 4:58:52 PM
simmons.232@osu.edu	COFILD	
df		
The Ohio State University		
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Jacob Harris Bane	CODIED	Sent: 11/18/2024 4:58:54 PM
bane.17@osu.edu	COPIED	
The Ohio State University		
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Kathryn Marie Reed	COPIED	Sent: 11/18/2024 4:58:55 PM
reed.901@osu.edu	COPILD	
The Ohio State University		
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Lisa N Delaney	CONTEN	Sent: 11/18/2024 4:58:57 PM
delaney.177@osu.edu	COPIED	
The Ohio State University		
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Maria N. Miriti	CODIED	Sent: 11/18/2024 4:58:58 PM
miriti.1@osu.edu	COPIED	
The Ohio State University		
Security Level: Email, Account Authentication (None)		
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Witness Events	Signature	Timestamp
	0	
Notary Events	Signature	Imestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	11/15/2024 9:22:38 AM
Certified Delivered	Security Checked	11/18/2024 4:58:14 PM
Signing Complete	Security Checked	11/18/2024 4:58:42 PM
Completed	Security Checked	11/18/2024 4:58:59 PM
Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, The Ohio State University (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact The Ohio State University:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows: To contact us by email send messages to: swisher.169@osu.edu

To advise The Ohio State University of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from The Ohio State University

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to esignature@osu.edu and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with The Ohio State University

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to swisher.169@osu.edu and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <u>https://support.docusign.com/guides/signer-guide-signing-system-requirements</u>.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify The Ohio State University as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by The Ohio State University during the course of your relationship with The Ohio State University.

ECE 5561: Introduction to Cybersecurity

Course Description

Introduction to cybersecurity. Technical fundamentals of data, software, component, network, and system security. Cybersecurity from an organizational and societal view point, including human factors.

Transcript Abbreviation: Intr Cybersecurity Grading Plan: Letter Grade Course Deliveries: Classroom, 100% at a distance, Greater or equal to 50% at a distance Course Levels: Undergrad, Graduate Student Ranks: Junior, Senior, Masters, Doctoral, Professional **Course Offerings:** Spring Flex Scheduled Course: Never **Course Frequency:** Every Year Course Length: 14 Week Credits: 3.0 **Repeatable:** No Time Distribution: 3.0 hr Lec Expected out-of-class hours per week: 6.0 Graded Component: Lecture Credit by Examination: No **Admission Condition: No Off Campus:** Never **Campus Locations:** Columbus Prerequisites and Co-requisites: Prerequisite: Junior, senior, or grad standing, or permission of instructor. Exclusions: Not open to student with credit for CSE 5471. Cross-Listings: Cross-listed with CSE 5471

Course Rationale: This course will serve as one of the foundational courses in the cybersecurity curriculum.

The course is required for this unit's degrees, majors, and/or minors: No The course is a GEC: No The course is an elective (for this or other units) or is a service course for other units: Yes

Subject/CIP Code: 14.0901 Subsidy Level: Doctoral Course

Programs

Abbreviation	Description
СрЕ	Computer Engineering
EE	Electrical Engineering

Course Goals

Become familiar with fundamental cybersecurity concepts, technologies and practices, and develop a foundation for further study in cybersecurity.

Become familiar with fundamentals of data security.

Become familiar with fundamentals of software security.

Become familiar with fundamentals of connection/network security.

Course Topics

Торіс	Lec	Rec	Lab	Cli	IS	Sem	FE	Wor
Basic concepts and definitions. Historical context. Cybersecurity frameworks.	3.0							
Data Security: Basic cryptography concepts, methods for data integrity and authentication, information storage security.	7.0							
Software security: software design with security requirements, testing, configuration management.	5.0							
Component security: Design, procurement, analysis, and maintenance of tangible components that are integrated into larger systems.	4.0							
Connection security: Security for networked systems, secure transmission models, common types of connection and transmission attacks.	5.0							
System security: System thinking, common system architectures, system management, access, control, and testing.	4.0							
Human security: identity management; personal awareness, understanding and compliance; human behavioral factors; personal data privacy and security.	3.0							
Organizational security: governance and policy strategies for organizations; cybersecurity risk management; legal and regulatory issues.	3.0							
Societal security: cybercrime, cyberlaw, cyberethics, cyberpolicy, privacy.	3.0							
Project presentations on complementary topics: hardware security, infrastructure security, cryptocurrencies etc.	5.0							

Representative Assignments

Case studies	
Final project	

Grades

Aspect	Percent
Assignments	30%
Midterm Exam	30%
Final project and presentation	40%

ABET-EAC Criterion 3 Outcomes

Course Contribution		College Outcome
	а	An ability to apply knowledge of mathematics, science, and engineering.
	b	An ability to design and conduct experiments, as well as to analyze and interpret data.
	c	An ability to design a system, component, or process to meet desired needs.
	d	An ability to function on multi-disciplinary teams.
	e	An ability to identify, formulate, and solve engineering problems.

Course Contribution		College Outcome	
	f	An understanding of professional and ethical responsibility.	
	g	An ability to communicate effectively.	
	h	The broad education necessary to understand the impact of engineering solutions in a global and societal context.	
	i	A recognition of the need for, and an ability to engage in life-long learning.	
	j	A knowledge of contemporary issues.	
	k	An ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.	

CpE ABET-EAC Criterion 9 Program Criteria Outcomes

Course Contribution		Program Outcome
*	1	an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics
	2	an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
*	3	an ability to communicate effectively with a range of audiences
**	4	an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
	5	an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives
	6	an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions
***	7	an ability to acquire and apply new knowledge as needed, using appropriate learning strategies

EE ABET-EAC Criterion 9 Program Criteria Outcomes

Course Contribution		Program Outcome
*	1	an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics
**	2	an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
*	3	an ability to communicate effectively with a range of audiences
**	4	an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
	5	an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives
	6	an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions
***	7	an ability to acquire and apply new knowledge as needed, using appropriate learning strategies

Additional Notes or Comments

Changed crosslinstg number to CSE 5471 $\,$ 11/20/20 BLA

Added CSE focuses too exclusions. 11/2420 BL

Prepared by: Irem Eryilmaz



Cybersecurity Law, Policy, and Management

PUBAFRS 5510 Spring, 2025

Course Information

- Course times:
- Credit hours: 3
- Mode of delivery: Online

Instructor

- Name:
- Email:
- Office hours:

Teaching Assistant

- Name:
- Email:
- Office Hours:

Why This Course is Important

The cybersecurity arms race means continual innovation in the kinds of threats posed to organizations. Cybersecurity policymakers and managers must also continually innovate. This innovation requires an integrated focus on the making and implementing of policy. Innovation is accelerated by breaking down the barriers caused by professional boundaries. Managers must understand their legal and policy responsibilities. Policymakers must understand the law to fully understand the gray areas of the law in which they can operate. The legal profession cannot continue to create laws that take superficial account of their policy and managerial implications.

The course provides the opportunity to see how technology, law, policy, and management interact through a framework that unites these perspectives. The framework also provides a more coherent way to approach layered cyber deterrence. In addition, the andragogical approach to teaching focuses on gaining understanding of abstract concepts through the effort of applying them to cases studies and fact patterns. An important element in the course design is to make use of scaffolding so that an integrated understanding can build incrementally with each module in the course.

Expectations of Undergraduate and Graduate Students

The course is designed to use scaffolding so that students continually build and refine their understanding each week from what was learned in previous weeks. Rather than eliminate any particular assignment, undergraduate students will have to answer less questions in the case studies, typically questions that rely on experience working in an organization.

COURSE OBJECTIVES

Goal: The goal of this course is to provide cybersecurity policymakers and managers with the legal, policy, and managerial concepts and tools to effectuate a coherent deterrence to cyber threats.

CONCEPTUAL OBJECTIVES

In successfully completing this course, a student will understand:

- The network of the U.S. institutions in cybersecurity policy and their roles and responsibilities.
- A working understanding of how public law operates to understand what legal responsibilities are in place and provide opportunities to participate effectively in the legal process.
- A working understanding of the relative strengths and weaknesses of "rule by fiat" versus "rule by persuasion" and an understanding of the skills necessary to manage through persuasion.
- The major ways that bureaucratic politics and intergovernmental and multisector coordination affect the creation and implementation of cybersecurity law
- Understand the basic components of federal and Ohio cybersecurity policy.

SKILL OBJECTIVES

In successfully completing this course, a student will have:

- A working skill in using an interdisciplinary framework that provides the capacity to understand what law can and cannot do, in light of policy, technical, and managerial constraints and opportunities.
- A developing skill in being able to recognize legal issues in fact patterns. This ability to frame a conversation and identify the issues will serve you well in your professional career.
- A rudimentary understanding of the basic tools in helping to interpret law.
- Basic legal research skills including how to find federal and state statutes, regulations, and case law.

Course Prerequisites

Students are expected to have taken ECE 5561: Introduction to Cybersecurity or PUBAFRS 5570 Data Governance in the public sector. Students can obtain a waiver through permission from the course instructor by having taken an equivalent course or by having prior experience.

How This Course Works

MODE OF DELIVERY

This is an online asynchronous course. Students are expected to do short readings / view recorded lectures and then apply that material to a problem. Typically, the application component involves some work done individually followed by a post or response to a post on a discussion board.

This course is divided into weekly modules that contain the materials you will need for that week. Navigating to each of these modules is the easiest way to find the materials you need and the directions for the class. The modules page is the first page you see when you log into the course website.

CREDIT HOURS AND WORK EXPECTATIONS

This is a three credit-hour course. According to <u>Ohio State bylaws on instruction</u> (Rule 3335-8-24 (A)(1)), students should expect around three hours per week on direct instruction in addition to six hours of homework (reading and assignment preparation, for example). The course has been designed so that you will be doing less than nine hours per week. If you are spending more than nine hours / week repeatedly, please let me know and I can help you use your time more efficiently or make adjustments in the assignments and / or readings.

ONLINE LECTURES

There will be recordings of class lectures to introduce the course readings by providing context for the material, explain more difficult concepts and skills, and how the material relates to what has been covered in the course and how it relates to future modules.

DISCUSSION BOARDS

Class participation points are earned through your participation on discussion boards. provide you with another way to earn class participation points. I use a mix of anonymous and non-anonymous discussion boards to encourage discussion, feedback, and class participation points. You can post something you found interesting in your personal reading, a follow-up question to what was discussed in class, or a comment on your peers' news presentation.

Discussion boards also provide you with a way to ask questions about class logistics. Questions might include, for example, on why a link is not working, about what is expected in an assignment, or where you should upload a file. This discussion board is anonymous.

Please note, that there is a high likelihood that if you have a question, others will have that same question. Discussion boards are sometimes a more effective way to deal with many questions because the whole class benefits from your question and our response. If you do have a question, we encourage you to use the discussion board if it is appropriate and if you feel comfortable in posting your question there. We can also respond to questions emailed to us.

Course Materials, Fees, and Technologies

REQUIRED READINGS

There is no required textbook. All required materials will be made available on the course website.

https://carmen.osu.edu

Once you have logged on to CARMEN you will see a link for this course. You will need to sign on to CARMEN using your OSU username.

COURSE TECHNOLOGY

For help with your password, university email, Carmen, or any other technology issues, questions, or requests, contact the OSU IT Service Desk. <u>https://it.osu.edu/help</u>

- Email: <u>mailto:8help@osu.edu</u>
- **Phone:** 614-688-HELP (4357)
- Self-Service and Chat support: <u>http://ocio.osu.edu/selfservice</u>
- **TDD:** 614-688-8743

BASELINE TECHNICAL SKILLS FOR ONLINE COURSES

- Basic computer and web-browsing skills
- Navigating Carmen: for questions about specific functionality, see the <u>Canvas</u> <u>Student Guide</u>. Additional navigation instructions are provided within the course.

REQUIRED TECHNOLOGY SKILLS SPECIFIC TO THIS COURSE

- CarmenZoom and text chat
- Recording, editing, and uploading video (explanations and instructions are provided on the course website)

REQUIRED EQUIPMENT

- Computer: current Mac (OS X) or PC (Windows 7+) with high-speed internet connection
- For office hours:
 - Webcam: built-in or external webcam, fully installed and tested
 - Microphone: built-in laptop or tablet mic or external microphone

REQUIRED SOFTWARE

 Microsoft Office 365: All Ohio State students are now eligible for free Microsoft Office 365 ProPlus through Microsoft's Student Advantage program. Full instructions for downloading and installation can be found at <u>go.osu.edu/office365help.</u>

CARMEN ACCESS

You will need to use <u>Buckeye Pass</u> multi-factor authentication to access your courses in Carmen.

If none of these options will meet the needs of your situation, you can contact the IT Service Desk at 614-688-4357 (HELP) and the IT support staff will work out a solution with you.

Course Expectations

If you are having difficulty with handling the course requirements because of COVID or other health and life challenges, please feel free to reach out and work with me.

EXPECTATIONS OF FACULTY AND TEACHING ASSISTANT

- Remember that you can call 614-688-4357 (HELP) at any time if you have a technical problem.
- Preferred contact method: If you have a question, please contact me first through my Ohio State email address. I will reply to emails within 24 hours on days when class is in session at the university and 48 hours on the weekend. I can also be reached by texting me at 614.795.6002.
- Lectures, activities, videos, practice quizzes, and other material will be posted online by **Wednesday morning for the next week**.
- Broken links or missing resources We try to check and recheck to make sure that links are working, but if you find a broken link, please let us know as soon as possible. You can earn one point for every broken link, erroneous date, or missing resource that is brought to the attention of the instructors through the logistics discussion board. The first person to identify the problem earns the point.

- Announcements: We use Announcements as the way to communicate with the class and to cut down on the number of emails that you receive. If you would like to have announcements sent as an email, you can adjust your notification settings. Please see <u>video</u> on how to manage your emails.
- Grading and feedback: You can generally expect feedback on your news assignments within the next 5 days to allow for timely and thoughtful feedback. Please allow for 7 days for feedback on your examinations and legal writing assignments.
- Class announcements: I will send all important class-wide messages through the Announcements tool in Carmen Canvas. Please check <u>your notification</u> <u>preferences</u> (go.osu.edu/canvas-notifications) to ensure you receive these messages.
- Discussion board: We will reply to messages on both the logistics discussion board and the content discussion board within 24 hours on school days. If you have a question about the course material or the logistics of the class, we prefer that you post the question on the appropriate discussion board first rather than as an email to us, so that everyone has a chance to hear your question and our response. Of course, you are still free to send us an email as not every question need be public.
- **There will be a midterm check-in** with you by using a course survey to see how the course is progressing. We would appreciate any suggestions on how we can improve your learning experience.

EXPECTATIONS OF STUDENTS

- Preparation for Class: Preparation includes reviewing lectures, activities, videos, practice quizzes, and possibly other material. Thus, satisfactory completion of this course requires you to actively engage with all online material. Treat this material as you would class time: take notes and formulate questions.
- Class Discussion: Class discussion is central to the discussion in a law course, so it is important that all students make their voices heard through discussion boards. There is one assignment that focuses on discussion board, but many of the class assignments will require individual preparation followed by a contribution or a response to a contribution to that assignment's discussion board.

Course Activities

Activity	Points	% of Final Grade
Class Participation	25	5%
Video introduction	(10)	
Professional Goals and Questions	(15)	
Early Feedback Quiz	25	5%
Mid-Term Examination	50	10%
Final Examination	100	20%
Discussion Board	25	5%
Identify appropriate technical, legal, political, managerial tools to address cybersecurity threat		
Case Studies	50	10%
1: Identify some of the critical cybersecurity issues facing organizations	(25)	
2: Participate in role play to understand rule-by-fiat versus rule-by-persuasion.	(25)	
Class Assignments	225	45%
1. Apply Integrating Framework to Better Identify critical issues in Case Study 1	(25)	
2. Identify legal authority of a regulation	(25)	
 Interpret regulation by application to a fact pattern 	(25)	
4. Write a simple regulatory rule	(25)	
 Revise rule taking into account theories of political control of bureaucracy. 	(25)	
6. Revise rule taking into account intergovernmental cooperation	(25)	

Activity	Points	% of Final Grade
7. Revise rule taking into account governance challenges (inter-sector cooperation.)	(25)	
8. High level scan of Ohio cybersecurity Policy. Grads: Speculate on management, intergovernmental and governance challenges not explicitly addressed.	(25)	
9. High level scan of Federal policy on data breaches. Grads: Speculate on management, intergovernmental and governance challenges not explicitly addressed.	(25)	
Total Possible Points	500	100%

Case Studies

Case Study 1: One important area for improving cybersecurity policy implementation is the coordination of policy and management across multisector and multigovernmental organizations. This case study will focus on a cybersecurity incident and understanding how to coordinate communications and activities. The case study will require knowing the various organizations having responsibility, the law relevant to the various organizations, and making sure that one's own organization has the capacity to work cooperatively.

Case Study 2: The second case study / role will provide an opportunity for students to learn how to manage by persuasion as well as by fiat. Given the multisector, multijurisdictional nature of preparing for a responding to cybersecurity threats, managing by fiat, issuing rules that are expected to be followed, is often not legally possible, or practically impossible. Students in this role play will be provided with a script that identifies their organization's interests, structure, budget, and technical capacity in addition to their legal and policy requirements. The case study prompt will be a growing awareness of a new kind of cybersecurity threat, and students are expected to codevelop a new protocol for dealing with those kinds of threats while considering their own needs as well as the public interest.

Class Assignments

Class Assignment 1: Revisit above Case Study 1 Fact Pattern and apply integrating framework to more thoroughly identify potential issues.

Class Assignment 2: Students are introduced to Legal Research tools: USCA, CFR and Nexis-Uni and asked to detail the flow of authority from Statutes, Regulations, and any important cases.

Class Assignment 3: Students will learn how to interpret and apply a DHS regulation that requires how a public organization should be prepared for cybersecurity threats.

Class Assignment 4: Once students have some experience reading law, this assignment requires students to write a regulation. This assignment will deepen their skill in interpreting law by understanding the competing pressures on how regulatory wording is chosen.

Class Assignment 5: Students are asked to refine earlier rule based upon reading the theory of political control of bureaucracy literature.

Class Assignment 6: Students are asked to refine a rule based upon reading the challenges to intergovernmental cooperation. Students now need to revisit a rule to acknowledge the challenge of intergovernmental relations.

Class Exercise 7: Students move from challenges to inter-organizational cooperation to inter-sector cooperation. Students now need to revisit rule to acknowledge governance challenges.

Class Exercise 8: Write up a short high-level summary of Ohio's Cybersecurity law. Speculate on implementation issues considering previous material on how public organizations work, intergovernmental relations, and governance.

Class Exercise 9: Write up a high-level summary of the Federal Government's Policy on data breaches. Speculate on implementation issues considering previous material on how public organizations work, intergovernmental relations, and governance.

Assigned Course Grade

А	100 to 93%	B-	< 83 to 80%	D+	< 70 to 67%
A-	< 93 to 90%	C+	< 80 to 77%	D	< 67 to 60%
B+	< 90 to 87%	С	< 77 to 73%	E	< 60%
В	< 87 to 83%	C-	< 73 to 70%		

Descriptions of Major Course Assignments

CLASS PARTICIPATION (75 POSSIBLE POINTS)

1. Introduce Yourself (5 possible points)

Please introduce yourself by uploading a video answering a couple of questions. Directions on how to create a video are included on the assignment page.

2. Explicitly identify career goals or career directions. Identify how this course can advance your professional development.

3. Class Discussion and Discussion Board (40 possible points)

Class participation is very important to this class. It is a public good.

Points	Grade	Criteria
35-40	A	Student frequently participates in class / discussion board and has thoughtfully commented on one news item before and after the midterm
30-34	A-	Student periodically participates in class / discussion board has commented thoughtfully on one news item
20-29	В	Student has participated in class in class / discussion board
10-19	С	Student attends classes hardly ever / never volunteers to participate
0-19	D-E	Student infrequently attends class

You will need to provide one comment on a news posting before the midterm and after the midterm to earn an "A" for class participation.

The discussion of law is not just a technical exercise. It involves policies, values, and political beliefs. My goal for the class is to have stimulating class discussion that includes diverse opinions. Good discussion rules allow these varying viewpoints to be expressed and respected. We will be developing ground rules for class discussion using a community discussion board.

EARLY FEEDBACK QUIZ (25 POINTS)

Description: There will be a short quiz on the fourth week of the class to give you feedback on how well you are doing with the course material. Please refer to previous

examinations available on the course website that can be found on the Learning Resources page.

Academic Integrity and collaboration: This is an individual assignment, and you cannot collaborate with others.

MID-TERM (50 POINTS) AND FINAL EXAMINATIONS (100 POINTS)

Description: All students are expected to take the examinations on the scheduled dates. If there is a scheduling conflict, exceptions *must* be discussed with the instructor *well in advance* of the examination. In the unlikely event of an emergency, please call or email as soon as it is convenient to do so, and we can make alternative arrangements. The final examination is cumulative, and you are responsible for all the material covered during the course, although relatively more of the questions will focus on the material covered since the midterm.

CLASS ASSIGNMENTS (225 points)

There are important "legal writing" skills in working with the law. Most of you will need these skills at some point during your professional life. One skill is reading cases. A second skill is in learning how to read and interpret statutes and rules. We will practice these skills during most our class sessions. There is a second set of skills that you will be graded on. These skills build upon the first set of skills through specific assignments. Please see the specific details in the assignment on the course website. Each of these assignments is worth twenty-five points.

All assignments are due by 11:59 pm on the due dates.

GRADE APPEALS

The assigned grade is designed to show the overall quality of work performed by each student. If you believe that any grade was not properly assigned you may write a letter explaining why you believe the grade was incorrectly assigned within one week of receiving the graded assignment back. Each appeal will be considered, and if a regrade is performed, the entire assignment will be re-graded. The final grade may be greater, less, or equal to the original grade.

Late Assignments

Late submissions are not accepted except for extenuating circumstances. If you have an extenuating circumstance, please contact me as soon as possible before the due date and we can work out an alternative due date.

Discussion and Communication Guidelines

The following are our expectations for how we should communicate as a class. Above all, please remember to be respectful and thoughtful. There is a discussion board for establishing our norms and practices that we will use for our professional communication.

- **Writing style**: While there is no need to participate on discussion boards as if you were writing a research paper, you should remember to write using good grammar, spelling, and punctuation so that you can be understood. A more conversational tone is fine for the discussions and peer feedback.
- Tone and civility: Let's maintain a supportive learning community where everyone feels safe and where people can disagree amicably. I am looking for disagreement but not uncivility. Remember that sarcasm doesn't always come across online. Learning requires a willingness to be vulnerable. We will not have great discussions if there is a negative tone or incivility in the class. We must be willing to risk asking what we fear might be a dumb question or when contributing our experience or insight. I have found that the best questions are not necessarily the most technical questions but those questions that we ask from the heart.
- Writing and backing up your work: Consider composing your academic posts in a word processor, where you can save your work, and then copying that material into the Carmen discussion.

Academic Integrity Policy

Academic integrity is essential to maintaining an environment that fosters excellence in teaching, research, and other educational and scholarly activities. Thus, The Ohio State University and the Committee on Academic Misconduct (COAM) expect that all students have read and understand the university's <u>Code of Student Conduct</u> (studentconduct.osu.edu), and that all students will complete all academic and scholarly assignments with fairness and honesty. Students must recognize that failure to follow the rules and guidelines established in the university's *Code of Student Conduct Conduct* and this syllabus may constitute "Academic Misconduct."

The Ohio State University's *Code of Student Conduct* (Section 3335-23-04) defines academic misconduct as: "Any activity that tends to compromise the academic integrity of the university or subvert the educational process." Examples of academic

misconduct include (but are not limited to) plagiarism, collusion (unauthorized collaboration), copying the work of another student, and possession of unauthorized materials during an examination. Ignorance of the university's *Code of Student Conduct* is never considered an excuse for academic misconduct, so I recommend that you review the *Code of Student Conduct* and, specifically, the sections dealing with academic misconduct.

If I suspect that a student has committed academic misconduct in this course, I am obligated by university rules to report my suspicions to the Committee on Academic Misconduct. If COAM determines that you have violated the university's *Code of Student Conduct* (i.e., committed academic misconduct), the sanctions for the misconduct could include a failing grade in this course and suspension or dismissal from the university.

If you have any questions about the above policy or what constitutes academic misconduct in this course, please contact me.

Other sources of information on academic misconduct (integrity) to which you can refer include:

RESOURCES FROM THE DRAKE INSTITUTE FOR TEACHING AND LEARNING RESOURCES FROM THE TEACHING AND LEARNING RESOURCE CENTER COMMITTEE ON ACADEMIC MISCONDUCT (COAM)

Artificial Intelligence and Academic Integrity

There has been a significant increase in the popularity and availability of a variety of generative artificial intelligence (AI) tools, including ChatGPT, Sudowrite, and others. These tools will help shape the future of work, research, and technology but when used in the wrong way, they can stand in conflict with academic integrity at Ohio State.

All students have important obligations under the <u>Code of Student Conduct</u> to complete all academic and scholarly activities with fairness and honesty. Our professional students also have the responsibility to uphold the professional and ethical standards found in their respective academic honor codes. Specifically, students are not to use unauthorized assistance in the laboratory, on field work, in scholarship or on a course assignment unless such assistance has been authorized specifically by the course instructor. In addition, students are not to submit their work without acknowledging any word-for-word use and/or paraphrasing of writing, ideas or other work that is not your own. These requirements apply to all students undergraduate, graduate, and professional.

In this class, please be sure to check for each assignment whether and how generative AI tools can be used to complete the assignment.

Creating an Environment Free from Harassment, Discrimination, and Sexual Misconduct

The Ohio State University is committed to building and maintaining a community to reflect diversity and to improve opportunities for all. All Buckeyes have the right to be free from harassment, discrimination, and sexual misconduct. Ohio State does not discriminate on the basis of age, ancestry, color, disability, ethnicity, gender, gender identity or expression, genetic information, HIV/AIDS status, military status, national origin, pregnancy (childbirth, false pregnancy, termination of pregnancy, or recovery therefrom), race, religion, sex, sexual orientation, or protected veteran status, or any other bases under the law, in its activities, academic programs, admission, and employment. Members of the university community also have the right to be free from all forms of sexual misconduct: sexual harassment, sexual assault, relationship violence, stalking, and sexual exploitation.

To report harassment, discrimination, sexual misconduct, or retaliation and/or seek confidential and non-confidential resources and supportive measures, contact the Office of Institutional Equity:

Online reporting form at <u>equity.osu.edu</u>, Call 614-247-5838 or TTY 614-688-8605, Or Email <u>equity@osu.edu</u>

The university is committed to stopping sexual misconduct, preventing its recurrence, eliminating any hostile environment, and remedying its discriminatory effects. All university employees have reporting responsibilities to the Office of Institutional Equity to ensure the university can take appropriate action:

- All university employees, except those exempted by legal privilege of confidentiality or expressly identified as a confidential reporter, have an obligation to report incidents of sexual assault immediately.
- The following employees have an obligation to report all other forms of sexual misconduct as soon as practicable but at most within five workdays of becoming aware of such information: 1. Any human resource professional (HRP); 2. Anyone who supervises faculty, staff, students, or volunteers; 3. Chair/director; and 4. Faculty member.

Diversity Statement

The Ohio State University affirms the importance and value of diversity of people and ideas. We believe in creating equitable research opportunities for all students and to providing programs and curricula that allow our students to understand critical societal challenges from diverse perspectives and aspire to use research to promote sustainable solutions for all. We are committed to maintaining an inclusive community that recognizes and values the inherent worth and dignity of every person; fosters

sensitivity, understanding, and mutual respect among all members; and encourages each individual to strive to reach their own potential. The Ohio State University does not discriminate on the basis of age, ancestry, color, disability, gender identity or expression, genetic information, HIV/AIDS status, military status, national origin, race, religion, sex, gender, sexual orientation, pregnancy, protected veteran status, or any other bases under the law, in its activities, academic programs, admission, and employment.

To learn more about diversity, equity, and inclusion and for opportunities to get involved, please visit:

https://odi.osu.edu/ https://odi.osu.edu/racial-justice-resources https://odi.osu.edu/focus-on-racial-justice https://cbsc.osu.edu

Glenn College Diversity Values Statement

The Glenn College is committed to nurturing a diverse and inclusive environment for our students, faculty, staff, and guests that celebrates the fundamental value and dignity of everyone by recognizing differences and supporting individuality. We are dedicated to creating a safe space and promoting civil discourse that acknowledges and embraces diverse perspectives on issues and challenges that affect our community.

Grievances and Solving Problems

A student who encounters a problem related to his/her educational program has a variety of avenues available to seek resolution. (Note: the procedures for grade grievances are explicitly covered in the faculty rules) Typically, a student is advised to resolve any dispute, disagreement, or grievance as directly as possible, engaging with the person or persons most closely involved. The faculty and staff of the departments and colleges are available to work with students in this regard. If this step does not produce acceptable results, the student should follow a logical stepwise progression to address the academic concerns.

According to University Policies, if you have a problem with this class, you should seek to resolve the grievance concerning a grade or academic practice by speaking first with the instructor or professor. Then, if necessary, take your case to the department chairperson, college dean or associate dean, and to the provost, in that order. Specific procedures are outlined in Faculty Rule 3335-8-23. Grievances against graduate, research, and teaching assistants should be submitted first to the supervising instructor, then to the chairperson of the assistant's department.

Your Mental Health

As a student you may experience a range of issues that can cause barriers to learning, such as strained relationships, increased anxiety, alcohol/drug problems, feeling down, difficulty concentrating and/or lack of motivation. These mental health concerns or stressful events may lead to diminished academic performance or reduce a student's ability to participate in daily activities. The Ohio State University offers services to assist you with addressing these and other concerns you may be experiencing.

If you or someone you know are suffering from any of the aforementioned conditions, you can learn more about the broad range of confidential mental health services available on campus via the Office of Student Life's Counseling and Consultation Service (CCS) by visiting <u>ccs.osu.edu</u> or calling 614-292-5766. CCS is located on the 4th floor of the Younkin Success Center and 10th floor of Lincoln Tower. You can reach an on-call counselor when CCS is closed at 614-292-5766 and 24-hour emergency help is also available through the 24/7 by dialing 988 to reach the Suicide and Crisis Lifeline.

Student Wellness

As a student, your health and wellness can have an impact on your academic success. Common wellness concerns during your time at the university may include high levels of stress, sleep and diet behaviors, alcohol and other drug use, depression and anxiety, and interpersonal relationship issues. The Office of Student Life has numerous resources and services available to you at no charge to help you address those concerns.

You can learn more about health and wellness resources available on campus by visiting the websites for the <u>Student Wellness Center</u>, <u>Wilce Student Health</u> <u>Center</u>, <u>Recreational Sports</u> and <u>Counseling and Consultation Service</u>. For students in recovery or seeking recovery from substance use disorders, learn more about support on campus by visiting the <u>Collegiate Recovery Community</u>. For students facing food insecurity, learn more about the free on-campus food pantry by visiting the <u>Buckeye</u> <u>Food Alliance</u>. For students interested in speaking with a peer to learn more about campus resources, call the <u>Buckeye Peer Access Line</u>. For students interested in meeting with a peer and setting holistic wellness goals, learn more about <u>Wellness</u> <u>Coaching</u>.

No Buckeye Goes Hungry

The Ohio State University is committed to ensuring that all students have access to adequate and healthy food. Any undergraduate or graduate student with a BuckID may

confidentially use the Buckeye Food Alliance food pantries. No proof of need is required. There are two locations:

- West Campus: Lincoln Tower. Doors are locked call 614-688-2508 upon arrival.
- North Campus: St. Stephens. Look for the Buckeye Food Alliance (BFA) sign on the southwest corner of the building.

To learn more, visit <u>https://www.buckeyefoodalliance.org/</u>

Disability Statement (with Accommodations for COVID)

The university strives to maintain a healthy and accessible environment to support student learning in and out of the classroom. If you anticipate or experience academic barriers based on your disability (including mental health, chronic, or temporary medical conditions), please let me know immediately so that we can privately discuss options. To establish reasonable accommodations, I may request that you register with Student Life Disability Services. After registration, make arrangements with me as soon as possible to discuss your accommodations so that they may be implemented in a timely fashion.

If you are isolating while waiting for a COVID-19 test result, please let me know immediately. Those testing positive for COVID-19 should refer to the Safe and Healthy Buckeyes site for resources. Beyond five days of the required COVID-19 isolation period, I may rely on Student Life Disability Services to establish further reasonable accommodations. You can connect with them at slds@osu.edu; 614-292-3307; or slds.osu.edu.

ACCESSIBILITY OF COURSE TECHNOLOGY

This online course requires use of CarmenCanvas (Ohio State's learning management system) and CarmenZoom and other online communication and multimedia tools. If you need additional services to use these technologies, please request accommodations with your instructor.

- <u>CarmenCanvas accessibility</u> (go.osu.edu/canvas-accessibility)
- Streaming audio and video
- <u>CarmenZoom accessibility</u> (go.osu.edu/zoom-accessibility)
- Collaborative course tools

Religious Accommodations

Ohio State has had a longstanding practice of making reasonable academic accommodations for students' religious beliefs and practices in accordance with applicable law. In 2023, Ohio State updated its practice to align with new state

legislation. Under this new provision, students must be in early communication with their instructors regarding any known accommodation requests for religious beliefs and practices, providing notice of specific dates for which they request alternative accommodations within 14 days after the first instructional day of the course. Instructors in turn shall not question the sincerity of a student's religious or spiritual belief system in reviewing such requests and shall keep requests for accommodations confidential.

With sufficient notice, instructors will provide students with reasonable alternative accommodations with regard to examinations and other academic requirements with respect to students' sincerely held religious beliefs and practices by allowing up to three absences each semester for the student to attend or participate in religious activities. Examples of religious accommodations can include, but are not limited to, rescheduling an exam, altering the time of a student's presentation, allowing make-up assignments to substitute for missed class work, or flexibility in due dates or research responsibilities. If concerns arise about a requested accommodation, instructors are to consult their tenure initiating unit head for assistance.

A student's request for time off shall be provided if the student's sincerely held religious belief or practice severely affects the student's ability to take an exam or meet an academic requirement **and** the student has notified their instructor, in writing during the first 14 days after the course begins, of the date of each absence. Although students are required to provide notice within the first 14 days after a course begins, instructors are strongly encouraged to work with the student to provide a reasonable accommodation if a request is made outside the notice period. A student may not be penalized for an absence approved under this policy.

If students have questions or disputes related to academic accommodations, they should contact their course instructor, and then their department or college office. For questions or to report discrimination or harassment based on religion, individuals should contact the <u>Office of Institutional Equity</u>.

Policy: Religious Holidays, Holy Days and Observances

FERPA and Privacy in CarmenZoom

Video and audio recordings of class lectures will be part of the classroom activity. The video and audio recordings are used for educational use/purposes and may be made available to all students presently enrolled in the course. Please note that you are not allowed to share these recordings. This is to protect your FERPA rights and those of your fellow students.

Course Schedule

Week	Subject	Concepts / Skills Covered	Readings	Assignments / Activities
1	Welcome to the Course	Course Syllabus		Case Study 1: Simple short fact pattern to generate interest and foreshadows some of the general themes in the course.
2	The Landscape – Intro to Integrating Framework showing the competing sets of values in cybersecurity	Technical* / Legal / Policy / Managerial Perspectives Framework	Rosenbloom's Separation of Powers article with the added dimension of technology	Class Assignment 1: Revisit above Fact Pattern and apply integrating framework to more thoroughly identify potential issues.
3	Overview of Administrative Law	(Relationship among Constitution, Statutes, Regulations, Criminal and Civil Law, Tort Law)	Reuse videos used in 6010 with the addition of comparing civil and criminal law	Class materials examine a regulation all the way from the authority found in the Constitution to Legislative Hearings, Statute, to Regulation, and challenges in Court. Early Feedback Quiz
4	Overview of Administrative Law	Deeper dive into rulemaking	Nutshell, "Administrative Rulemaking"	Class Assignment 2: Students are introduced to Legal Research tools.
5	How Law Works	Students learn how to interpret law	Legal Writing primer on legal interpretation	Class Assignment 3: Now that students know how to look up a regulation, students are asked to find the regulation and interpret the rule as it applies to a fact pattern provided in the assignment.
6	How Law Works	Students better understand law by writing a rule	Legal Writing primer on writing a rule	Class Assignment 4: Given a fact pattern provided in an assignment, students are asked to write a rule to deal with that fact pattern.
7	Midterm			Open-book essay question
8	Public Organizations: An Information Processing Model	The course will use an "organization as brain" or "information flows" as a metaphor for how to manage and create policy	Galbraith (Revisit) Primer on Data Governance Rules	Discussion Board Assignment 1: Use integrating framework, identify appropriate set of technical, legal, political, and managerial tools to deal with cybersecurity threat.
9	Fiat and Persuasion	Case Study 1 (readings on negotiation)	One article on new tools for governance; one reading on doing multiparty negotiation	Case study 2: Through two rounds of moves, this second case study will provide an opportunity for students to learn how to manage by persuasion and influence.
Week	Subject	Concepts / Skills Covered	Readings	Assignments / Activities
------	-----------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------
9	How Public Organizations Work I	While administrative agencies write and administer the law, a lot of law is written through its implementation. What are the on-the-ground factors that affect implementation? (Theories of Political Control of Bureaucracy)	Buffat (2015) Street- Level Bureaucracy and E-Government; de Boer and Raaphorst (2023) Automation and discretion: explaining the effect of automation on how street-level bureaucrats enforce SLBs	Class Assignment 5: Students are asked to refine earlier rule based upon reading the literature on the political control of bureaucracy.
10	How Public Organizations Work II	Intergovernmental Relations	Peters and Pierre (2001) "Developments in intergovernmental relations: towards multi- level governance"	Class Exercise 6: Students are asked to refine rule based upon reading the challenges to intergovernmental cooperation
11	How Public Organizations Work III	Governance Theory and Public Administration	Vigoda (2002) "From responsiveness to collaboration: governance, citizens, and the next generation of public administration"	Class Exercise 7: Students move from challenges to inter-organizational cooperation to inter-sector cooperation.
12	Application	Evaluate Ohio's Cybersecurity Policy Framework	O.R.C. 125.18 ; DAS ITS-SEC-02 Policy Private Sector issues addressed by Guest Interview with Ohio Adjutant General	Class Exercise 8: Write up a high-level summary of Ohio's Cybersecurity law.
13	Application	Evaluate Federal Government's Policy with respect to interorganizational coordination with Private Sector, State and Local governments	Federal requirements on reporting of data breaches (or the real lack thereof)	Class Exercise 9: Write up a high-level summary of the Federal Government's Policy on data breaches.
14	Final Exam Review			Class Discussion Board seeded with questions from instructor to review important concepts and concepts not well-understood.
15	Final Exam			



Data Governance for Public Organizations

PUBAFRS 5570 Spring, 2025

Course Information

- Course times:
- Credit hours: 3
- Mode of delivery: Online

Instructor

- Name:
- Email:
- Office hours:

Teaching Assistant

- Name:
- Email:
- Office Hours:

Course Description

This course is an introductory examination of data governance using cybersecurity as a case study. Access to data is essential to making informed decisions. Data governance, therefore, is central to the success of public sector organizations. As organizations mature technologically, professionals understanding data governance will have an important tool in their professional toolkit.

Many of the concepts and skills in this course focus upon cybersecurity and other public sector issues, but these concepts and skills are just as important to private and

non-profit organizations. Students from outside of the John Glenn College of Public Affairs are welcome to join the class.

The public sector has the most important role in organizing efforts in dealing with cybersecurity threats. Cybersecurity breaches involve breaking criminal and civil law and even pose threats to U.S. national security. Creating appropriate policy and implementing these policies requires a multi-sector, multi-organizational response, especially where there are strong incentives to not publicize cybersecurity breaches or reveal how those breaches occurred.

Students routinely learn application of concepts through in-class exercises, casestudies, and a table-top simulation exercise. The course begins with a working knowledge on risk management and systems analysis. The course then covers core data governance concepts including Data Governance Frameworks, Data Security, Information Quality, Data Modeling and Design, and management of organizations and individuals.

Why This Course is Important

Influenced by recent technological achievements, popular wisdom describes our century as the "Information Age." Yet, far too little explicit attention is devoted to formally governing data. Data governance answers the question "who gets what information in what form and for what use." This definition spans the range of issues as organizations manage their data flows, from the mundane questions about the costs of collecting and storing data, to how well the organization supports individuals in understanding and using data in decision-making, cybersecurity threats, and the larger policy questions of where and how to manage bias in algorithms, and the due process threats coming from increasing automation of organizational processes.

Rather than relying on a central explicit organizational focus on data management, most organizations rely on managers of individual projects to be responsible for managing their data. The consequences, however, is that the collective needs of the whole organization or the larger enterprise is overlooked or compromised. A reliance on individual project-based responsibility usually often results in little to no effective data management techniques.

The consequences of poor data management can mean poor quality information, data not being available when it is needed for a decision, less than useful information, efficiency costs, decisions made without the benefit of quality information, inappropriate uses of data, and threats to privacy and cybersecurity.

Cybersecurity will serve as a major theme of the course since it is important threat to organizations, and often competes with other concerns organizations face, for example, the transparency and the easy flow of information within and across organizations to support decision-making more effectively.

Expectations of Undergraduate and Graduate Students

Undergraduate students are expected to complete all the weekly assignments, while Graduate Students are also required to complete the semester long case study. Undergraduate students will write a 10-page paper on a subject of their choosing.

COURSE OBJECTIVES

Goal: The goal of this course is to provide students with the concepts and skills to effectively govern data with a focus on managing cybersecurity risks.

CONCEPTUAL OBJECTIVES

In successfully completing this course, a student will understand:

- An interdisciplinary framework that balances competing legal, managerial, policy, and technological mandates by applying them to case studies and homework assignments.
- Basic information governance principles as measured by being able to apply these ideas to case studies and homework assignments. These concepts include:
 - Risk Management and Layered Cyber Deterrence
 - Data and Information Lifecycle Management
 - Standards-setting bodies and processes
 - Metadata and the Semantic Web
 - Information Quality Assessment
 - Data Governance Implementation Success Factors

SKILL OBJECTIVES

In successfully completing this course, a student will be able to:

- Develop a rudimentary data governance framework with a focus on managing cybersecurity threats
- Conduct a basic systems analysis to support developing a data governance plan
- Beginner-level skills in assessing tradeoffs between managing cybersecurity threats and fulfilling other organizational needs for data.

Course Prerequisites

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.

How This Course Works

MODE OF DELIVERY

This is an online asynchronous course where course materials in the form of readings, lectures are provided online.

This course is divided into weekly modules that contain the materials you will need for that week. Navigating to each of these modules is the easiest way to find the materials you need and the directions for the class. The modules page is the first page you see when you log into the course website.

CREDIT HOURS AND WORK EXPECTATIONS

This is a 3 credit-hour course. According to <u>Ohio State bylaws on instruction</u> (Rule 3335-8-24 (A)(1)), students should expect to work around twelve hours per week. The amount of time in each week will vary, but I do not believe you will be devoting twelve hours / week to this class. If you are spending more than twelve hours / week repeatedly, please let me know and I can help you use your time more efficiently.

ONLINE LECTURES

There will be recordings of class lectures to introduce the course readings by providing context for the material, explain more difficult concepts and skills, and how the material relates to what has been covered in the course and how it relates to future modules.

DISCUSSION BOARDS

Class participation points are earned through discussion boards. The courses use a mix of anonymous and non-anonymous discussion boards to encourage discussion, feedback, and class participation points.

Discussion boards also provide a way to ask questions about class logistics. Questions might include, for example, on why a link is not working, about what is expected in an assignment, or where you should upload a file. This discussion board is anonymous. Please note, that there is a high likelihood that if you have a question, others will have that same question. Discussion boards are sometimes a more effective way to deal with many questions because the whole class benefits from your question and our response. If you do have a question, we encourage you to use the discussion board if it is appropriate and if you feel comfortable in posting your question there. We can also respond to questions emailed directly to us.

Course Materials, Fees, and Technologies

REQUIRED READINGS

There is only one required textbook: DAMA International (2017). Data Management Book of Knowledge (2d Ed.) Technics Publications, Basking Ridge N.J. ISBN 9-871-634622-349 (Paperback).

Students can access textbook information via the Barnes & Noble bookstore website: <u>www.shopOhioState.com</u> as well as from their BuckeyeLink Student Center. This information is disseminated by B&N to all area bookstores. **You may buy from a** store of your choice and/or shop for books (always use ISBN# for searches) online.

Additional readings, case studies and exercises are provided through the course website on CARMEN:

https://carmen.osu.edu

Once you have logged on to CARMEN you will see a link for this course. You will need to sign on to CARMEN using your OSU username.

COURSE TECHNOLOGY

For help with your password, university email, Carmen, or any other technology issues, questions, or requests, contact the OSU IT Service Desk. <u>https://it.osu.edu/help</u>

- o Email: mailto:8help@osu.edu
- **Phone:** 614-688-HELP (4357)
- Self-Service and Chat support: <u>http://ocio.osu.edu/selfservice</u>
- **TDD:** 614-688-8743

BASELINE TECHNICAL SKILLS FOR ONLINE COURSES

- Basic computer and web-browsing skills
- Navigating Carmen: for questions about specific functionality, see the <u>Canvas</u> <u>Student Guide</u>. Additional navigation instructions are provided within the course.

REQUIRED TECHNOLOGY SKILLS SPECIFIC TO THIS COURSE

- o CarmenZoom and text chat
- Recording, editing, and uploading video (explanations and instructions are provided on the course website)

REQUIRED EQUIPMENT

- Computer: current Mac (OS X) or PC (Windows 7+) with high-speed internet connection
- For office hours:
 - o Webcam: built-in or external webcam, fully installed and tested
 - Microphone: built-in laptop or tablet mic or external microphone

REQUIRED SOFTWARE

 Microsoft Office 365: All Ohio State students are now eligible for free Microsoft Office 365 ProPlus through Microsoft's Student Advantage program. Full instructions for downloading and installation can be found at <u>go.osu.edu/office365help.</u>

CARMEN ACCESS

You will need to use <u>Buckeye Pass</u> multi-factor authentication to access your courses in Carmen.

If none of these options will meet the needs of your situation, you can contact the IT Service Desk at 614-688-4357 (HELP) and the IT support staff will work out a solution with you.

Course Expectations

If you are having difficulty with handling the course requirements because of COVID or other health and life challenges, please feel free to reach out and work with me.

EXPECTATIONS OF FACULTY AND TEACHING ASSISTANT

- Remember that you can call 614-688-4357 (HELP) at any time if you have a technical problem.
- Preferred contact method: If you have a question, please contact me first through my Ohio State email address. I will reply to emails within 24 hours on days when class is in session at the university and 48 hours on the weekend. I can also be reached by texting me at 614.795.6002.
- Lectures, activities, videos, practice quizzes, and other material will be posted online by **Wednesday morning for the next week**.
- Broken links or missing resources We try to check and recheck to make sure that links are working, but if you find a broken link, please let us know as soon as possible. You can earn one point for every broken link, erroneous date, or missing resource that is brought to the attention of the instructors through the logistics discussion board. The first person to identify the problem earns the point.
- **Announcements**: We use Announcements as the way to communicate with the class and to cut down on the number of emails that you receive. If you would like to have announcements sent as an email, you can adjust your notification settings. Please see <u>video</u> on how to manage your emails.
- Grading and feedback: You can generally expect feedback on your news assignments within the next 5 days to allow for timely and thoughtful feedback. Please allow for 7 days for feedback on your examinations and legal writing assignments.
- Class announcements: I will send all important class-wide messages through the Announcements tool in Carmen Canvas. Please check <u>your notification</u> <u>preferences</u> (go.osu.edu/canvas-notifications) to ensure you receive these messages.
- Discussion board: We will reply to messages on both the logistics discussion board and the content discussion board within 24 hours on school days. If you have a question about the course material or the logistics of the class, we prefer that you post the question on the appropriate discussion board first rather than as an email to us, so that everyone has a chance to hear your question and our

response. Of course, you are still free to send us an email as not every question need be public.

• **There will be a midterm check-in** with you by using a course survey to see how the course is progressing. We would appreciate any suggestions on how we can improve your learning experience.

EXPECTATIONS OF STUDENTS

- During the Week: Students are expected to review video lectures, activities, videos, practice quizzes, and possibly other material. Thus, satisfactory completion of this course requires you to actively engage with all online material. Treat this material as you would class time: take notes and formulate questions.
- Class Discussion: Class discussion is central to the discussion, so it is important that all students make their voices heard through discussion boards. At the end of each class period, I will make note of which students contributed to the class discussion. At the end of the semester, these classroom participation points along with points earned from your online discussion will be totaled and given a grade using the rubric found in this syllabus. Each contribution made during the class is worth one hash mark. Each contribution to any discussion board is worth two hash points.

You are being evaluated against the schedule and whether there is a clear pattern of contribution. I am not comparing individuals against one other. If everyone contributes to the class discussion, you could all earn an "A" for class participation.

Activity	Points	% of Final Grade
I. Class Participation	90	20%
1. Video introduction	(5)	
2. Discussion Board	(50)	
3.	(25)	
II. Early Feedback Quiz	20	5%
III. Case Studies	200	50%
1. Cybersecurity- Identify Issues	(20)	
2. Model Information Flows	(40)	
3.	(40)	
4. Threats to Data Quality	(20)	
5. Create a Data Model	(40)	
6. Applying Law to Data Management Project	(20)	
7. Design a Cybersecurity Data Governance Framework	(40)	
V. Individual Project / Paper	100	25%
Total Possible Points	400	100%

Course Activities

Descriptions of Major Course Assignments

I. Class Participation

1. Video Introductions – Please introduce yourselves to the rest of the class. The course will make use of group work within and outside of the class.

2. Discussion Boards - Questions about the readings or case studies will serve as another way to engage the student in the course material. Please see rubric for how class participation will be graded.

3. Constructive Feedback on Individual Presentations – Students are expected to review presentation materials before class and make constructive suggestions on the data governance plans and the presentation itself. Materials will be provided on how to provide constructive feedback including

how to evaluate the quality of the presentations. Students should use the project rubric to evaluate the quality of the data governance plans.

Points	Grade	Criteria
35-40	A	Student frequently participates in class discussion boards.
30-34	A-	Student periodically participates in discussion board.
20-29	В	Student has participated in class discussion board.
10-19	С	Student hardly ever participates in discussion board.
0-19	D-E	Student never participates in discussion board.

Class participation is very important to this class. It is a public good.

II. Early Feedback Quiz – A short quick quiz on the concepts to-date will provide quick feedback to the student on their progress in the course. Results of the quiz will be administered before the deadline by which students can drop the course without loss of significant tuition costs.

III. Case Studies - The class makes extensive use of case studies. Case studies are useful tools to learn what are sometimes abstract concepts by applying them to the real world.

Case Study 1: This case study will introduce data governance through the lens of managing data through a cybersecurity lens. You are required to identify potential data management problems. The case study also requires you to apply a risk management to identify both the salience of the risk and a layered cyber deterrence plan using appropriate policy, technical, and managerial measures to manage that risk. The case study is rich in detail and serves to foreshadow future concepts to be discussed in the course. As such, the class will continue to "mine" this case study for future insights on how to manage data.

Case Study 2: A very important foundational concept in data management is that of "data flows." Rather than seeing the operation of an organization through an organization chart, data managers see organizations as "data flows" so that they can make sure that the right information gets to the right person for an appropriate use. When this applies to cybersecurity, the data manager focuses on how data may get to the wrong person for the wrong use. Students learn how to use systems analysis as a way to formally model these flows.

"OCAP Systems Analysis case study." Future case studies will build upon the work in this case study.

One important area for improving cybersecurity policy implementation is the coordination policy and management across multisector and multigovernmental units. This case study will focus on knowing the law on which institutions should be involved, how they should be contacted, where the responsibilities lie and making sure that one's own organization has the capacity to work cooperatively.

Case Study 3: This case study requires you to develop a detailed data model of the Client – Case relationship in the OCAP case study.

Case Study 4: Using OCAP Case study data dictionary, identify metadata to manage cybersecurity. Emphasis will be placed on creating interoperability of this metadata with other organizations.

Case Study 5: Use the OCAP systems analysis to identify possible threats to information quality. The focus will be the threats that poor quality pose to managing cybersecurity risk. You are required to first develop appropriate metadata for a data dictionary. Students are then required to conduct a quality assessment of a small subset of data within the data dictionary using quality rule templates.

Case Study 6: Students will learn how to interpret and apply the statute and DHS regulations that assign responsibilities and processes attendant to data breaks. Students must understand the organization's and individual' responsibilities and develop policy and procedures that identify the nature and the severity of the breach and a communication plan. The analysis should also include a mechanism to learn from the experience.

Case Study 7: Students are provided with a local organization's data management governance framework. Students will provide a high-level memorandum identifying the important elements of a data governance framework and a process by which the organization can plan and manage the innovation in the construction of this framework.

IV. Individual Class Project / Undergrad Paper - Beginning with week 3, students will work on their own individual class project and apply the knowledge and skills to cumulatively build their individual project. A detailed description of a "quasi-real" organization will be provided. Students are then expected to use an integrating framework of law, management, policy, and technology that allows for a systematic data governance evaluation. Instead of completing a class project, undergraduate students are required to complete a ten page paper on a data governance topic of their choosing. Student should work with the instructor on refining their paper topic.

(Future iterations of this assignment may allow students to focus on their own organization's cybersecurity programs.)

Assigned Course Grade

A	100 to 93%	B-	< 83 to 80%	D+	< 70 to 67%
A-	< 93 to 90%	C+	< 80 to 77%	D	< 67 to 60%
B+	< 90 to 87%	С	< 77 to 73%	E	< 60%
В	< 87 to 83%	C-	< 73 to 70%		

All assignments are due by 11:59 pm on the above due dates.

GRADE APPEALS

The assigned grade is designed to show the overall quality of work performed by each student. If you believe that any grade was not properly assigned you may write a letter explaining why you believe the grade was incorrectly assigned within one week of receiving the graded assignment back. Each appeal will be considered, and if a regrade is performed, the entire assignment will be re-graded. The final grade may be greater, less, or equal to the original grade.

Late Assignments

Late submissions are not accepted except for extenuating circumstances. If you have an extenuating circumstance, please contact me as soon as possible before the due date and we can work out an alternative due date.

Discussion and Communication Guidelines

The following are our expectations for how we should communicate as a class. Above all, please remember to be respectful and thoughtful. There is a discussion board for establishing our norms and practices that we will use for our professional communication.

- **Writing style**: While there is no need to participate on discussion boards as if you were writing a research paper, you should remember to write using good grammar, spelling, and punctuation so that you can be understood. A more conversational tone is fine for the discussions and peer feedback.
- **Tone and civility**: Let's maintain a supportive learning community where everyone feels safe and where people can disagree amicably. I am looking for disagreement but not uncivility. Remember that sarcasm doesn't always come

across online. Learning requires a willingness to be vulnerable. We will not have great discussions if there is a negative tone or incivility in the class. We must be willing to risk asking what we fear might be a dumb question or when contributing our experience or insight. I have found that the best questions are not necessarily the most technical questions but those questions that we ask from the heart.

• Writing and backing up your work: Consider composing your academic posts in a word processor, where you can save your work, and then copying that material into the Carmen discussion.

Academic Integrity Policy

Academic integrity is essential to maintaining an environment that fosters excellence in teaching, research, and other educational and scholarly activities. Thus, The Ohio State University and the Committee on Academic Misconduct (COAM) expect that all students have read and understand the university's <u>Code of Student Conduct</u> (studentconduct.osu.edu), and that all students will complete all academic and scholarly assignments with fairness and honesty. Students must recognize that failure to follow the rules and guidelines established in the university's *Code of Student Conduct*."

The Ohio State University's *Code of Student Conduct* (Section 3335-23-04) defines academic misconduct as: "Any activity that tends to compromise the academic integrity of the university or subvert the educational process." Examples of academic misconduct include (but are not limited to) plagiarism, collusion (unauthorized collaboration), copying the work of another student, and possession of unauthorized materials during an examination. Ignorance of the university's *Code of Student Conduct* is never considered an excuse for academic misconduct, so I recommend that you review the *Code of Student Conduct* and, specifically, the sections dealing with academic misconduct.

If I suspect that a student has committed academic misconduct in this course, I am obligated by university rules to report my suspicions to the Committee on Academic Misconduct. If COAM determines that you have violated the university's *Code of Student Conduct* (i.e., committed academic misconduct), the sanctions for the misconduct could include a failing grade in this course and suspension or dismissal from the university.

If you have any questions about the above policy or what constitutes academic misconduct in this course, please contact me.

Other sources of information on academic misconduct (integrity) to which you can refer include:

RESOURCES FROM THE DRAKE INSTITUTE FOR TEACHING AND LEARNING RESOURCES FROM THE TEACHING AND LEARNING RESOURCE CENTER COMMITTEE ON ACADEMIC MISCONDUCT (COAM)

Artificial Intelligence and Academic Integrity

There has been a significant increase in the popularity and availability of a variety of generative artificial intelligence (AI) tools, including ChatGPT, Sudowrite, and others. These tools will help shape the future of work, research, and technology but when used in the wrong way, they can stand in conflict with academic integrity at Ohio State.

All students have important obligations under the <u>Code of Student Conduct</u> to complete all academic and scholarly activities with fairness and honesty. Our professional students also have the responsibility to uphold the professional and ethical standards found in their respective academic honor codes. Specifically, students are not to use unauthorized assistance in the laboratory, on field work, in scholarship or on a course assignment unless such assistance has been authorized specifically by the course instructor. In addition, students are not to submit their work without acknowledging any word-for-word use and/or paraphrasing of writing, ideas or other work that is not your own. These requirements apply to all students undergraduate, graduate, and professional.

In this class, please be sure to check for each assignment whether and how generative AI tools can be used to complete the assignment.

Creating an Environment Free from Harassment, Discrimination, and Sexual Misconduct

The Ohio State University is committed to building and maintaining a community to reflect diversity and to improve opportunities for all. All Buckeyes have the right to be free from harassment, discrimination, and sexual misconduct. Ohio State does not discriminate on the basis of age, ancestry, color, disability, ethnicity, gender, gender identity or expression, genetic information, HIV/AIDS status, military status, national origin, pregnancy (childbirth, false pregnancy, termination of pregnancy, or recovery therefrom), race, religion, sex, sexual orientation, or protected veteran status, or any other bases under the law, in its activities, academic programs, admission, and employment. Members of the university community also have the right to be free from all forms of sexual misconduct: sexual harassment, sexual assault, relationship violence, stalking, and sexual exploitation.

To report harassment, discrimination, sexual misconduct, or retaliation and/or seek confidential and non-confidential resources and supportive measures, contact the Office of Institutional Equity:

Online reporting form at <u>equity.osu.edu</u>, Call 614-247-5838 or TTY 614-688-8605, Or Email <u>equity@osu.edu</u> The university is committed to stopping sexual misconduct, preventing its recurrence, eliminating any hostile environment, and remedying its discriminatory effects. All university employees have reporting responsibilities to the Office of Institutional Equity to ensure the university can take appropriate action:

- All university employees, except those exempted by legal privilege of confidentiality or expressly identified as a confidential reporter, have an obligation to report incidents of sexual assault immediately.
- The following employees have an obligation to report all other forms of sexual misconduct as soon as practicable but at most within five workdays of becoming aware of such information: 1. Any human resource professional (HRP); 2. Anyone who supervises faculty, staff, students, or volunteers; 3. Chair/director; and 4. Faculty member.

Diversity Statement

The Ohio State University affirms the importance and value of diversity of people and ideas. We believe in creating equitable research opportunities for all students and to providing programs and curricula that allow our students to understand critical societal challenges from diverse perspectives and aspire to use research to promote sustainable solutions for all. We are committed to maintaining an inclusive community that recognizes and values the inherent worth and dignity of every person; fosters sensitivity, understanding, and mutual respect among all members; and encourages each individual to strive to reach their own potential. The Ohio State University does not discriminate on the basis of age, ancestry, color, disability, gender identity or expression, genetic information, HIV/AIDS status, military status, national origin, race, religion, sex, gender, sexual orientation, pregnancy, protected veteran status, or any other bases under the law, in its activities, academic programs, admission, and employment.

To learn more about diversity, equity, and inclusion and for opportunities to get involved, please visit:

https://odi.osu.edu/ https://odi.osu.edu/racial-justice-resources https://odi.osu.edu/focus-on-racial-justice https://cbsc.osu.edu

Glenn College Diversity Values Statement

The Glenn College is committed to nurturing a diverse and inclusive environment for our students, faculty, staff, and guests that celebrates the fundamental value and dignity of everyone by recognizing differences and supporting individuality. We are dedicated to creating a safe space and promoting civil discourse that acknowledges and embraces diverse perspectives on issues and challenges that affect our community.

Grievances and Solving Problems

A student who encounters a problem related to his/her educational program has a variety of avenues available to seek resolution. (Note: the procedures for grade grievances are explicitly covered in the faculty rules) Typically, a student is advised to resolve any dispute, disagreement, or grievance as directly as possible, engaging with the person or persons most closely involved. The faculty and staff of the departments and colleges are available to work with students in this regard. If this step does not produce acceptable results, the student should follow a logical stepwise progression to address the academic concerns.

According to University Policies, if you have a problem with this class, you should seek to resolve the grievance concerning a grade or academic practice by speaking first with the instructor or professor. Then, if necessary, take your case to the department chairperson, college dean or associate dean, and to the provost, in that order. Specific procedures are outlined in Faculty Rule 3335-8-23. Grievances against graduate, research, and teaching assistants should be submitted first to the supervising instructor, then to the chairperson of the assistant's department.

Your Mental Health

As a student you may experience a range of issues that can cause barriers to learning, such as strained relationships, increased anxiety, alcohol/drug problems, feeling down, difficulty concentrating and/or lack of motivation. These mental health concerns or stressful events may lead to diminished academic performance or reduce a student's ability to participate in daily activities. The Ohio State University offers services to assist you with addressing these and other concerns you may be experiencing.

If you or someone you know are suffering from any of the aforementioned conditions, you can learn more about the broad range of confidential mental health services available on campus via the Office of Student Life's Counseling and Consultation Service (CCS) by visiting <u>ccs.osu.edu</u> or calling 614-292-5766. CCS is located on the 4th floor of the Younkin Success Center and 10th floor of Lincoln Tower. You can reach an on-call counselor when CCS is closed at 614-292-5766 and 24-hour emergency help is also available through the 24/7 by dialing 988 to reach the Suicide and Crisis Lifeline.

Student Wellness

As a student, your health and wellness can have an impact on your academic success. Common wellness concerns during your time at the university may include high levels of stress, sleep and diet behaviors, alcohol and other drug use, depression and anxiety, and interpersonal relationship issues. The Office of Student Life has numerous resources and services available to you at no charge to help you address those concerns.

You can learn more about health and wellness resources available on campus by visiting the websites for the <u>Student Wellness Center</u>, <u>Wilce Student Health</u> <u>Center</u>, <u>Recreational Sports</u> and <u>Counseling and Consultation Service</u>. For students in recovery or seeking recovery from substance use disorders, learn more about support on campus by visiting the <u>Collegiate Recovery Community</u>. For students facing food insecurity, learn more about the free on-campus food pantry by visiting the <u>Buckeye</u> <u>Food Alliance</u>. For students interested in speaking with a peer to learn more about campus resources, call the <u>Buckeye Peer Access Line</u>. For students interested in meeting with a peer and setting holistic wellness goals, learn more about <u>Wellness</u> <u>Coaching</u>.

No Buckeye Goes Hungry

The Ohio State University is committed to ensuring that all students have access to adequate and healthy food. Any undergraduate or graduate student with a BuckID may confidentially use the Buckeye Food Alliance food pantries. No proof of need is required. There are two locations:

- West Campus: Lincoln Tower. Doors are locked call 614-688-2508 upon arrival.
- North Campus: St. Stephens. Look for the Buckeye Food Alliance (BFA) sign on the southwest corner of the building.

To learn more, visit https://www.buckeyefoodalliance.org/

Disability Statement (with Accommodations for COVID)

The university strives to maintain a healthy and accessible environment to support student learning in and out of the classroom. If you anticipate or experience academic barriers based on your disability (including mental health, chronic, or temporary medical conditions), please let me know immediately so that we can privately discuss options. To establish reasonable accommodations, I may request that you register with Student Life Disability Services. After registration, make arrangements with me as soon as possible to discuss your accommodations so that they may be implemented in a timely fashion. If you are isolating while waiting for a COVID-19 test result, please let me know immediately. Those testing positive for COVID-19 should refer to the Safe and Healthy Buckeyes site for resources. Beyond five days of the required COVID-19 isolation period, I may rely on Student Life Disability Services to establish further reasonable accommodations. You can connect with them at slds@osu.edu; 614-292-3307; or slds.osu.edu.

ACCESSIBILITY OF COURSE TECHNOLOGY

This online course requires use of CarmenCanvas (Ohio State's learning management system) and CarmenZoom and other online communication and multimedia tools. If you need additional services to use these technologies, please request accommodations with your instructor.

- <u>CarmenCanvas accessibility</u> (go.osu.edu/canvas-accessibility)
- Streaming audio and video
- <u>CarmenZoom accessibility</u> (go.osu.edu/zoom-accessibility)
- Collaborative course tools

Religious Accommodations

Ohio State has had a longstanding practice of making reasonable academic accommodations for students' religious beliefs and practices in accordance with applicable law. In 2023, Ohio State updated its practice to align with new state legislation. Under this new provision, students must be in early communication with their instructors regarding any known accommodation requests for religious beliefs and practices, providing notice of specific dates for which they request alternative accommodations within 14 days after the first instructional day of the course. Instructors in turn shall not question the sincerity of a student's religious or spiritual belief system in reviewing such requests and shall keep requests for accommodations confidential.

With sufficient notice, instructors will provide students with reasonable alternative accommodations with regard to examinations and other academic requirements with respect to students' sincerely held religious beliefs and practices by allowing up to three absences each semester for the student to attend or participate in religious activities. Examples of religious accommodations can include, but are not limited to, rescheduling an exam, altering the time of a student's presentation, allowing make-up assignments to substitute for missed class work, or flexibility in due dates or research responsibilities. If concerns arise about a requested accommodation, instructors are to consult their tenure initiating unit head for assistance.

A student's request for time off shall be provided if the student's sincerely held religious belief or practice severely affects the student's ability to take an exam or

meet an academic requirement **and** the student has notified their instructor, in writing during the first 14 days after the course begins, of the date of each absence. Although students are required to provide notice within the first 14 days after a course begins, instructors are strongly encouraged to work with the student to provide a reasonable accommodation if a request is made outside the notice period. A student may not be penalized for an absence approved under this policy.

If students have questions or disputes related to academic accommodations, they should contact their course instructor, and then their department or college office. For questions or to report discrimination or harassment based on religion, individuals should contact the <u>Office of Institutional Equity</u>.

Policy: <u>Religious Holidays, Holy Days and Observances</u>

FERPA and Privacy in CarmenZoom

Video and audio recordings of class lectures will be part of the classroom activity. The video and audio recordings are used for educational use/purposes and may be made available to all students presently enrolled in the course. Please note that you are not allowed to share these recordings. This is to protect your FERPA rights and those of your fellow students.

Course Schedule

Subject	Concepts / Skills Covered	Readings and Assignments
Introduction to Data Management and Governance		
1. Foundational Concepts	Risk Management, Layered Cyber Deterrence	R: Cyberspace Solarium Commission Report, March 2020, Executive Summary; R Tsokas et al (2021) Risk Management for Business Process Reengineering: The Case of a Public Sector Organization. Case Study 1: Cybersecurity case study to apply risk management and cyber deterrence concepts and foreshadow future course modules
2. The Larger Context of Data Governance	Data Governance Framework; Data Architecture, Systems Analysis	R: DMBOK, Chapter 1, pp. 17-31; DMBOK, Chapter 3 Case Study 2: Use OCAP DB systems analysis case study and formally model information flows using conventional systems analysis modeling tools
Core Concepts and Skills		
3. Data Modeling and Design	Building Data Models and Using Data Modeling Tools	R: DMBOK Chapter 5 Case Study 3: Using OCAP DB case study data dictionary and conceptual model, develop a data model of Client–Case relationship
4. Data Security	Organization Data Security Requirements; Assessing Tradeoffs between Cybersecurity and Other Business Drivers	DMBOK, Chapter 4, pp. 217-248 Individual Class Project Assignment: Using Data Security Requirements Checklist in DMBOK, begin to identify gaps for Individual Data Project Guest Speaker: Ted Stanich (Alumnus) DHS / EPA Early Feedback Quiz
5. Data Security, Round 2	Data Security Policy, and Security Standard	DMBOK, Chapter 7, pp. 256-266

Subject	Concepts / Skills	Readings and Assignments
Managing Projects	Covered	
6. Document and Content Management	Lifecycle Management, Enterprise Content Management Systems	DMBOK, Chapter 9
7. Metadata Management	Semantic Web; Metadata Architecture; Standards-setting bodies and processes,	R: DMBOK, Chapter 12 Case Study 4: Using OCAP Case study data dictionary, identify metadata to manage cybersecurity
8. Data / Information Quality	Data Profiling Tools, Quality Assessment, Quality Rule Templates	R: DMBOK Chapter 13 Case Study 5: Use OCAP systems analysis to identify possible threats to information quality
9. Going from Law and Policy to Implementation	Admin Law and Management; Tools and Guides for Legal Interpretation	YouTube Video: "Overview of Admin Law" YouTube Video: Interpreting the Law: A Guide for the Professional Case Study 6: Interpret Statute - Regulatory Rule – Executive Order and develop organizational capacity and management plan to implement rule
10. Governance and Organizational Change Management	Implementation Success Factors, Innovation Management	R: DMBOK, Chapter 17 R: Cinar et al (2019) A systematic review of barriers to public sector innovation process Case Study 7: Create a data governance framework and a process by which the organization can further plan and manage the innovation in construction of a cybersecurity data management plan.
11. Data Governance, Data Science and Al	Defining Big Data / AI and Business Needs	R: DMBOK, Chapter 14 R: EDM Council: "Eyes on Data: Importance of Data Governance When Implementing AI/ML"
12. Work on Data Governance Project)	(No new material. Time is provided to work with instructor on data governance project)	No class, work on your data governance project
1314. Present Data Governance Project	How to Give Effective Feedback How to Make an Effective Presentation	
15. Finalize Governance Project		No class, based upon class feedback, finalize your governance project. Indicate how you responded to suggestions.

MSL Data Privacy and Cybersecurity Regulation and Compliance

Fall 2023

Live Discussion/Office Hours: 5:00 pm – 7:30 pm (I don't know which Mondays OSU has scheduled these. I agreed to three over the 10 weeks)

Room – Virtual/Asynchronous

Professor Kirk Herath 614-286-9841 | <u>kirk.herath@gmail.com</u>

Office Hours: By appointment. Email questions are also welcomed.

Zoom Meeting ID: 969 1745 4851

Course Overview

This course examines the legal, policy, and operational management issues related to individual privacy and data protection. Privacy is a rapidly developing area of law as governments, businesses and society respond to the growing challenges and risks regarding the protection of information about an identified or identifiable individual. Data privacy law affects a vast range of businesses and products including social media, 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 professional's role within the corporate environment, touching on the various aspects a data privacy function has on legal and compliance, information technology, human resources, information security, corporate communications, and internal audit. Students will learn to apply privacy legal frameworks across sectors and to assess privacy 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, developing a privacy policy, and drafting data security and privacy contractual provisions.

This course will provide the student with the ability to:

- Understand the role of the privacy lawyer and professional in ensuring compliance with privacy legal frameworks regarding the collection and use of data across multiple sectors.
- · Identify major issues raised by Federal and state data privacy laws and regulations and develop policy responses to them.
- Identify and understand the general requirements of the EU's General Data Protection Rule (GDPR) and evaluate its effects on U.S. based privacy compliance programs.

- Identify and understand the major issues involved in civil and criminal enforcement of data privacy regulations.
- Understand and apply the core privacy management principles to key business operations.
- · Identify the key legal and ethical challenges encountered by privacy professionals.

Required Texts and Other Materials

The required text for this course is Lothar Determann's "Field Guide to Data Privacy Law". It is a very good companion to read along with tailored class readings. My advice is to use it to understand terms and topics, such as consent, notice, etc. It's also a resource that you can use once you're practicing law. It's available on Amazon.

The book that I edited, Herath, "Building a Privacy Program: A Practitioner's Guide", was published by the International Association of Privacy Professionals (IAPP). Unfortunately, it is out of print, but I will be copying and posting relevant sections of it throughout the semester in advance of each class in an online place Moritz provides for me. If you can find a used copy on Amazon or other book seller sites, snatch it up. While it's a little out of date concerning newer laws and regulations (since it was published in 2011), it is a wonderful OPERATIONAL resource for "practitioners" on how to build a program. All of that material, as well as the overview of laws prior to 2011, are still very good.

Additional required readings for each class will consist of open-source materials and excerpts from selected texts. Hyper links or citation to these materials are provided in the syllabus.

Participation

Class participation is expected through discussion posts. Students will be rewarded for exceptionally intelligent participation.

Class Assignments and Grading

There will be discussion and assignments associated with each module. You will need to complete these by Sunday evening at 11:59 p.m. each week to receive full credit. Each assignment is worth 100 points and discussion posts are worth 50 points each. There will be a potential 1350 points over the course of the class.

Barring extraordinary circumstances, assignments submitted outside the permitted time frame without a pre-approved extension will not be accepted.

Grading

This course follows the grading scale and grading policies outlined in the academic standards policy.

Other Important Policies and Statements are in the Appendix Below following the Class descriptions, learning objectives and reading assignments

Module 1: Course Overview and Fair Information Practices (FIPs)

This class covers key concepts in the field of data protection, privacy and security. It provides an detailed week by week overview of materials that we will cover this semester, including all assignments and expectations. We will also discuss topics for the short paper and timelines.

You will learn the scope and sources of data protection laws, the kinds of data protected and which regulators oversee data protection. Further you will learn about resources to stay abreast of privacy law and and how the ever-evolving field of data privacy impacts business, government and society.

Learning Objectives are to:

- Understand modern history of privacy.
- · Describe personal data.
- Understand data protection rules.
- Understand modern privacy frameworks.

Readings

- Robert Gelman, "Fair Information Practices: A Basic History", available at https://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf
- Cate, "The Failure of Fair Information Practice Principles," (especially section 4 "A Modest Proposal.") (2006), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972
- Hartzog, "The Inadequate, Invaluable Fair Information Practices," 76 Maryland Law Review 952 (2017), available at <u>https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3759&context</u> =mlr or <u>https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3017312</u>.
- Skim Steven Chabinskyu and Paul Pittman, "USA: Data Protection Laws and Regulations 2020," available at: <u>https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa</u>

Discussion Instructions – peer review at least three of your peers' postings.

Assignment – Discuss FIPPS and how it can be useful to any privacy or legal professional to issue spot a specific fact pattern.

Module 2: California and Other State Comprehensive Privacy Laws

This class continues our discussion of U.S. state data privacy and security laws with a focus on the trend towards more comprehensive consumer data privacy laws initiated by the California Consumer Privacy Act (CCPA). While California started the current trend of state-based

comprehensive privacy laws, lawyers and companies must contend with several other states, including laws enacted in Virginia and Colorado. In addition to these several other states have passed similar laws comprising a growing and fairly uniform set of data privacy law.

Learning Objectives are to:

- Explain how state data privacy laws are evolving.
- · Identify the main requirements of the California Consumer Privacy Act (CCPA) and the changes made by the California Privacy Rights Act (CPRA), and understand the differences in the new set of other state comprehensive privacy laws.
- Apply key requirements of the CCPA to a corporate privacy notice and other data practices.

Reading

- California Consumer Privacy Act of 2018, original text plus legislative amendments to date, available at https://theCCPA.org/
- THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020, available at https://oag.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20-Version%203%29_1.pdf
- Kosseff, "Ten Reasons why California's New Data Protection Law is Unworkable, Burdensome, and Possibly Unconstitutional" (July 9, 2018), available at <u>https://blog.EricGoldman.org/archives/2018/07/ten-reasons-why-Californias-new-data-protection-law-is-unworkable-burdensome-and-possibly-unconstitutional-guest-blog-post.him</u>
- Colorado: Colorado Privacy Act, available at https://leg/Colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_enr.pdf
- Virginia: Virginia Consumer Data Protection Act, available at <u>https://lis.Virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf</u>
- IAPP State Proposed Law Comparison Chart, available at, <u>https://iapp.org/resources/article/us-state-privacy-legislation-tracker/</u>
- Jessani, "What California, Colorado and Virginia Teach Us About the Future of US Privacy Law, " (InfoSecurity Magazine Oct 5, 2021), available at <u>https://www.wilmerhale.com/en/insights/publications/20211005-what-California-Colorado-and-Virginia-teach-us-about-the-future-of-us-privacy-law</u>

Discussion Instructions

- 1. Complete your analysis of the <u>Nationwide Insurance Privacy Notice for California</u> <u>Residents</u>.
- 2. Post your analysis with any questions you have about whether/how the Notice complies with the California Consumer Privacy Act.

Your initial post is due **Thursday at 11:59pm ET** with 2 additional responses to your peers, posted no later than **Sunday at 11:59pm ET**. Please remember this is a post first discussion. You must post your initial post before seeing replies.

Assignment Instructions

- 1. Read *The Score's privacy notice analyzed against the CCPA*. This article provides a detailed example of how to apply the CCPA to an existing privacy policy.
- 2. Read Nationwide Insurance's Privacy Notice for California Residents.
- Using the article above and the <u>checklist on this site</u>, draft your own analysis of how Nationwide's Privacy Notice complies with the CCPA. We recognize that this is a challenging assignment. Don't worry about getting it 100% perfect. Just do your best. We will provide feedback in the follow-up discussion.
- 4. Use .5 inch margins, Arial or Calibri, 12-point font. Submit your completed assignment by **Thursday at 11:59pm ET**.

Module 3: Data Breach Notification

We will learn about the variety of data breach requirements – statutory and regulatory — in the United States. This will include a look at the patchwork of state breach laws, the way Federal regulators backed into the space, as well as how state attorneys general have impacted business practices.

Learning objectives are to:

- Understand the U.S. state/federal framework
- Apply the law to a practical fictional client opinion assignment (case study)

Readings

• California Data Breach Notification Law, California Civil Code, Section 1798.82, available

at <u>https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.</u> 82.&lawCode=CIV

- Federal Trade Commission, "Data Breach Response, A Guide For Business", available at <u>https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business</u>
- Mitnick, "No more waiting: it's time for a federal data breach law in the U.S.," available at <u>https://www.accessnow.org/no-more-waiting-its-time-for-a-federal-data-breach-law-in-the-u-s/</u> (April 10, 2018)

- Obama Administration, "The Personal Data Notification & Protection Act," <u>https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/upd</u> <u>ated-data-breach-notification.pdf</u>
- 45 C.F.R. § 164.402 (Definitions) Breach
- Federal Trade Commission, "Statement of the Commission On Breaches by Health Apps and Other Connected Devices," (Sept. 15, 2021), available at <u>https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf</u>

Discussion Instructions

1. Complete the Data Breach Notification Assignment.

2. Post your analysis and, using one of the differences you identified in each law, explain what you think the likely effect and rationale is for that difference.

Your initial post is due **Thursday at 11:59pm ET** with 2 additional responses to your peers, posted no later than **Sunday at 11:59pm ET**. Please remember this is a post first discussion. You must post your initial post before seeing replies.

Assignment Instructions

- 1. Read the following fact pattern regarding a potential data breach.
- 2. Skim <u>Data-Security-Breach-Notice-Letter.pdf</u> and refer to it as a resource for your post.
- 3. Re-read the California and Ohio data breach notification laws and draft a brief analysis comparing the following issues under each law: (1) whether this incident is a reportable breach (including any additional information you think you need to decide; (2) the timing for sending the notification under each law; and (3) the information you would include in the notification letter.
- 4. Use .5 inch margins, Arial or Calibri, 12-point font. Submit your completed assignment by **Thursday at 11:59pm ET**.

Fact Pattern

On June 19, 2020, MEDNAX discovered that an unauthorized third party gained access to certain Microsoft Office 365-hosted MEDNAX business email accounts through phishing. "Phishing" occurs when an email is sent that looks like it is from a trustworthy source, but it is not. The phishing email prompts the recipient to share or give access to certain information. Upon discovery of this event, MEDNAX immediately took action to prevent any further unauthorized activity, began an investigation, and engaged a national forensic firm.

Based on the investigation, the unauthorized party was able to access certain business email accounts between June 17, 2020 and June 22, 2020.

The event was limited to a small number of business email accounts. Those email accounts are separate from MEDNAX's internal network and systems, which were not involved in the event. Even though a thorough investigation was conducted, it was not possible to conclusively determine whether personal information was actually accessed by the unauthorized party. No information was exfiltrated from any account. Based on the data analysis that was performed and ultimately completed in late November 2020, we were able to determine that over 1000 individuals may have had the following information in the email accounts:

- 1. first and last name; and
- 2. security code for accessing online health portal.

Module 4: FCRA and the FACT Act

This class surveys the Fair Credit Reporting Act (FCRA) and the FACT Act, which amended and updated the FCRA. These two laws are major federal sectoral privacy law governing the collection and use of consumer report information (i.e., credit reports). We will discuss how consumer report information is regulated by both state AGs and the FTC.

Learning objectives are to:

- · Identify and apply the major provisions of the FCRA and FACT Act.
- Understand and describe how consumer reports are created and how consumer reporting agencies are regulated.
- Describe how consumer reports can be legally used by creditors and employers.

Readings

- Federal Trade Commission, "A Summary of Your Rights Under the Fair Credit Reporting Act," available at <u>https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf</u>
- Consumer Financial Protection Bureau, "Exam Manual Update," available at <u>https://files.consumerfinance.gov/f/documents/102016_cfpb_GLBAExamManualUpdate.</u> <u>pdf</u> (Read pages 1-7)

Discussion – Post your written analysis and peer review at least three of your classmates' analysis.

Assignment – Everyone is permitted to obtain access to their consumer reports. Go online and look at your credit report from at least two consumer reporting agencies (Experian,

TransUnion or Equifax). Describe the ease or not of the process for obtaining your consumer report, checking your report for any innacurracies and, if there are any begin the correction process. Also, describe the process surrounding your ability to limit access, opt-out, freeze or control who can use your consumer report. Do not put your credit score in this analysis, but it would be interesting to know whether or not you understand the score.

Module 5: Financial Services Privacy and Security - Gramm-Leach-Bliley Act (GLBA)

This class surveys GLBA, which is a major federal sectoral privacy law governing the financial services industry. We will discuss how privacy for financial services is regulated by both state and federal regulators.

Learning objectives are to:

- · Identify and apply the major provisions of the GLBA.
- Understand and describe the common features and differences among these laws and the FTC's Section 5 authority.

Readings

- Hoofnagle, Hartzog and Solove, "The FTC can rise to the privacy challenge, but not without help from Congress," available at <u>https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacychallenge-but-not-without-help-from-Congress/</u>
- Federal Trade Commission, "How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act," (July 2002). Available at: https://www.ftc.gov/system/files/documents/plain-language/bus67-how-to-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf

Discussion – Post your written assignment and peer review three classmates' posts.

Assignment – Describe what financial services companies are required to do under under GLBA and list out the different regulators (both state and federal) and which industries they regulate.

Module 6: HIPAA and HITECH

We will read and review how the health care sector is regulated by the Health Insurance Portability and Accountability Act (HIPAA) and the related Health Information Technology for Economic and Clinical Health Act (HITECH).

Learning Objectives are to:

• Identity the major provisions of the HIPAA and HITECH.

Readings

- Nahra, "HIPAA Privacy and Security for Beginners," available at https://www.wileyrein.com/newsroom-newsletters-item-5029.html
- 45 C.F.R. Section 164.501(Definitions) "treatment," "payment" and "health care operations"
- 45 C.F.R. Section 164.501(Definitions) "covered entity," "health care provider," and "health plan" (skim the health plan definition)
- 45 C.F.R. Section 164.501(Definitions) Marketing
- 45 C.F.R. § 164.502(a)
- 45 C.F.R. § 164.506
- 45 C.F.R. § 164.508
- 45 C.F.R. §164.512 (skim, focus on topics addressed rather than details)
- 45 C.F.R. § 160.103 (Definitions) "Business Associate"
- 45 C.F.R. § 164.504e (Business Associate Contracts)
- Nahra, "A public service announcement about the HIPAA Privacy Rule," (IAPP), June 21, 2021, available at https://www.wilmerhale.com/en/insights/publications/20210621-a-public-service-announcement-about-the-hipaa-privacy-rule
- SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS, available at <u>https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html</u>

Assignment Description

You are the General Counsel and/or Chief Compliance Officer for NewCorp. NewCorp is a holding company containing a diverse array of affiliates and subsidiaries. NewCorp produces computer equipment for commercial and retail customers. It also owns a bank, mortgage company an insurance company. Finally, it has recently announced a new health tech cloud data service to help pharmacies manage customer information. NewCorp has the full array of web and digital properties on which you sell and service your customers. They also have some in-person retail operations. NewCorp is a U.S. domiciled company with HQ's in Birmingham, Alabama, and operates in all 50 states.

- Your assignment as GC/CCO is to analyze NewCorp's business and recommend:
- 1. How many privacy statements are needed?
- 2. How would each need to be communicated to customers and consumers?
- 3. Which privacy laws cover NewCorp's business activities?
- 4. Which regulators have jurisdiction over each of NewCorp's privacy compliance activities.
- Use .5 inch margins, Arial or Calibri, 12-point font. Submit your completed assignment by **Thursday at 11:59pm ET**.

Module 7: EU General Data Protection Regulation (GDPR)

In this module we will survey the European approach to data privacy or data protection with a focus on the General Data Protection Regulation and representative national implementing legislation and its impact on data transfers, particularly to and from the U.S.

Learning Objectives are to:

- · Identify and explain the key concepts of Europeans data protection law,
- Identify and explain the major provisions of the General Data Protection Regulation (GDPR) and its relationship to national implementing legislation in European countries.

Readings

- Information Commissioner's Office, "Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now," available at <u>https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/03/preparing-for-the-gdpr-12-steps.pdf</u> (and other locations)
- Philip L. Gordon, "Ten Steps For U.S. Multinational Employers Towards Compliance With Europe's New Data Protection Framework – The General Data Protection Regulation," available at <u>http://www.littler.com/publication-press/publication/ten-steps-us-multinational-employers-towards-compliance-europe%E2%80%99s-new</u>
- Solove, "Why I Love the GDPR: Ten Reasons," (May 2, 2018), available at https://teachprivacy.com/why-i-love-the-gdpr/.
- Lomas, "EU puts out final guidance on data transfers to third countries," (TechCrunch June 22, 2021, available at <u>https://techcrunch.com/2021/06/22/eu-puts-out-final-guidance-on-data-transfers-to-third-countries/</u>
- Allen & Overy, The EU General Data Protection Regulation, available at <u>http://www.allenovery.com/publications/en-gb/data-protection/Documents/GDPR-Brochure-2018.pdf</u>

You should also review relevant sections of Determann's Field Guide, as he nicely synthesizes all of the requirements.

Discussion Instructions

- One of the more challenging aspects of the GDPR is determining a lawful basis for processing personal data. Read the article <u>Direct Marketing Under the GDPR: Consent vs</u> <u>Legitimate Interests</u>, which discusses how two of the most commonly used bases potentially apply to direct marketing to consumers.
- 2. Explain what each of these bases require for direct marketing to consumers and the pros and cons of relying on each.

Your initial post is due **Thursday at 11:59pm ET** with 2 additional responses to your peers, posted no later than **Sunday at 11:59pm ET**. Please remember this is a post first discussion. You must post your initial post before seeing replies.

Module 8: The Federal Trade Commission and Privacy and Security Protection

The U.S. lacks a comprehensive national data privacy law. Instead, it has a patchwork of laws and regulations that apply to specific sectors and/or activities, including consumer protection, health-care, financial services, and others. The Federal Trade Commission (FTC) has interpreted its authority to protect consumers against "unfair and deceptive" trade practices to encompass requiring companies to engage in reasonable security and privacy practices.

Learning Objectives are to:

- Understand and describe the role of the Federal Trade Commission in regulating data security and privacy.
- Explain how the FTC has interpreted Section 5 of the Federal Trade Commission Act to provide authority to regulate data security and privacy.
- Understand and describe the limits of the FTC's authority and why it relies primarily on enforcement actions instead of formal rule-making to regulate data security and privacy.

Readings

- The Federal Trade Commission, "Start with Security: A Guide for Business," available at <u>https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business</u>.
- The Federal Trade Commission, "Financial Institutions and Customer Information: Complying with the Safeguards Rule", available at <u>https://www.ftc.gov/tips-</u> advice/business-center/guidance/financial-institutions-customer-information-complying.
- The Federal Trade Commission, "Standards for Safeguarding Customer Information; Final Rule," (16 CFR Part 314)(May 23, 2002) available at: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standardssafeguarding-customer-information-16cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf (Read the actual provisions of the Rule at 36493-36494)
- Section 5 of the FTC Act. Available here and in other places. <u>HTTPS://www.law.Cornell.edu/us code/text/15/45</u> (focus on (a)(1) and (a)(4)
- LabMD v. Federal Trade Commision, Case No. 16-16270 (11th Cir. 2018), available at http://media.ca11.UScourts.gof/opinions/pub/files/201616270.pdf.

Discussion – Post your assignment and peer review at least three of your classmates' posts.

Assignment – Analyze the LabMD case and whether or not you agree with the court's ultimate holding and whether or not this case sets a good standard for what comprises "reasonable" security.

Module 9: TCPA and the FCC (and the FTC and State Attorneys General)

This class will be a discussion of the Telephone Consumer Protection Act of 1991 (TCPAP, which is another federal sectoral privacy law. We discuss the the role of the Federal Communications Commission, which is the primary regulator, and we will also discuss the roles of the FTC and state AGs in enforcement.

Learning Objectives are to:

- Understand and apply the major provisions of the Telephone Consumer Protection Act (TCPA).
- Explain the important Federal privacy enforcement role played by the Federal Communications Commission.
- Will add a few state do not call laws and article on the importance of state AG enforcement

Readings

• Electronic Privacy Information Center, "Telemarketing and the Telephone Consumer Protection Act (TCPA)," available at <u>https://www.epic.org/privacy/telemarketing</u> / (skip past "Top News" to Introduction)

Discussion – Post your assignment and peer review at least three classmates' posts.

Assignment – Investigate the process for putting your name on both the Federal and the Ohio do not call lists. Describe the process and whether or not you put your name on those lists.

Module 10: COPPA and CAN-SPAM

We discuss the Children's Online Privacy Protection Act (COPPA) and the CAN-SPAM Act, the Telephone Consumer Protection Act of 1991 and the role of the Federal Communications Commission.

Learning Objectives are to:

- Understand and apply the major provisions of COPPA.
- · Understand and apply the major provisions of the CAN-SPAM Act.
- Explain the important Federal privacy enforcement role played by the Federal Trade Commission.

Readings

- Federal Trade Commission, Complying with COPPA, <u>https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0</u>
- Federal Trade Commission, "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business," available at <u>https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance</u>
- Proposed new legislation on COPPA (Press release), available at https://castor.house.gov/news/documentsingle.aspx?DocumentID=403677
- [Proposed] STIPULATED ORDER FOR PERMANENT INJUNCTION AND CIVIL PENALTY JUDGMENT (Google and YouTube), available at <u>https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order.pdf</u>
- 5 U.S.C. §7704(a)(3), (a)(4) (CAN-SPAM Act)
- Federal Trade Commission, "CAN-SPAM Act: A Compliance Guide For Business," available at https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business
- Brennan, Complying with the CAN-SPAM Act (2016), available at <u>https://www.lexisnexis.com/lexis-practice-advisor/the-</u> journal/b/lpa/archive/2016/11/08/complying-with-the-can-spam-act.aspx
- Wodinsky, "The Butt Pajamas Will Follow You Forever," (Dec. 20, 2020), available at https://gizmodo.com/the-butt-pajamas-will-follow-you-forever-1845929307
- Federal Trade Commission, "COMPLYING WITH COPPA: FREQUENTLY ASKED QUESTIONS," available at <u>https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0</u>

Discussion – Post your assignment and peer review at least three of your classmates' posts.

Assignment – Provide examples from your own personal email account of marketing emails and describe the process for removing yourself from marketing. Review the online terms and conditions of at least three companies and how their processes compare and contrast for ease of consumer preference management and control over marketing and sharing of consumer information.

Appendix – Additional Important Policies and Statements

Disability

Moritz is committed to providing an environment that ensures that no individual is discriminated against on the basis of disability. In light of the current pandemic, students seeking to request COVID-related accommodations may do so through the University's <u>request process</u>, managed by Student Life Disability Services. If you anticipate or experience academic barriers based on your disability (including mental health, chronic, or temporary medical conditions), you should notify Assistant Dean for Students Darren Nealy as soon as possible at 614-688-4676 or <u>nealy.1@osu.edu</u>. Dean Nealy will work with you and Student Life Disability Services to coordinate reasonable accommodations for students with documented disabilities. Student Life

Disability Services contact information: <u>slds@osu.edu</u>; 614-292-3307; 098 Baker Hall, 113 W. 12th Avenue.

Academic Misconduct

Academic integrity is essential to maintaining an environment that fosters excellence in teaching, research, and other educational and scholarly activities. The Ohio State University and the College of Law expect that all students have read and understand the Moritz College of Law Honor Code and that all students will complete all academic and scholarly assignments and examinations in compliance with the Honor Code. Students must recognize that failure to follow the rules and guidelines established in the Honor Code and this syllabus may constitute academic misconduct as defined in Article IV.B of the Honor Code. Examples of academic misconduct include (but are not limited to) plagiarism, collusion (unauthorized collaboration), copying the work of another student, and possession of unauthorized materials during an examination. Ignorance of the Honor Code is never considered an excuse for academic misconduct, so I recommend that you review the Honor Code. If I suspect that a student has committed academic misconduct in this course, I am obligated by College rules to report my suspicions to the College Administration. The sanctions for the misconduct could include a failing grade in this course, suspension or dismissal from the College and University, and a report to the relevant bar authorities. If you have any questions about the above policy or what constitutes academic misconduct in this course, please contact me.

Attendance

I expect regular and punctual in-person class attendance and preparation for class, in conformity with the requirements of College Rule 9.08 and ABA Standard 308. I reserve the right to sanction a failure to meet these expectations by exclusion from the course in question, by reduction in course grade, or by memorandum to a student's file.

Students are expected to follow University requirements for COVID-19 quarantine and isolation, as well all public health guidance from state, federal, and local authorities. You should notify me as soon as possible if you are unable to attend class for medical reasons (COVID-19 or other illnesses), or for emergency or similar reasons. Students in special situations or those requiring accommodation should seek support from Student Life Disability Services and/or Assistant Dean for Students Darren Nealy.

Class recordings

Video and/or audio recordings of class lectures and discussions will be part of this course. The video and audio recording(s) will be used for educational purposes and may be made available to all students presently enrolled in the course. Students are not permitted to create recordings of all or any part of any class, whether by video, photographic, audio, or any other means (including computer screenshots). Students are not permitted to share any recordings of all or any part of any class, whether by video, photographic, audio, or any other means (including computer screenshots). Making, using, or sharing recordings of this class in any form constitutes a
violation of Rule 9.33 of the Moritz Faculty Rules and of the Ohio State University Code of Student Conduct and will be handled administratively within the College. Violation of this policy may be sanctioned by exclusion from the course, by reduction in the course grade, or by memorandum to a student's file (which may be reported to relevant bar authorities).

Mental Health

As a student you may experience a range of issues that can cause barriers to learning, such as strained relationships, increased anxiety, alcohol/drug problems, feeling down, difficulty concentrating and/or lack of motivation. These mental health concerns or stressful events may lead to diminished academic performance or reduce a student's ability to participate in daily activities. The Ohio State University and the Moritz College of Law offer services to assist you with addressing these and other concerns you may be experiencing. Moritz students have access to our embedded counselor, <u>Audia Fraley</u>, as well as <u>urgent care</u> and <u>triage counseling</u>, provided from the University. Both the <u>Wexner Medical Center</u> and the <u>Ohio State Chief Wellness</u> <u>Officer</u>have made available helpful mental health online resources specific to the coronavirus pandemic.

You can learn more about the broad range of confidential mental health services available on campus via the Office of Student Life Counseling and Consultation Services (CCS) by visiting <u>ccs.osu.edu</u> or calling (614) 292- 5766. CCS is located on the 4th Floor of the Younkin Success Center and 10th Floor of Lincoln Tower. You can reach an on-call counselor when CCS is closed at (614) 292-5766 and 24 hour emergency help is also available through the 24/7 National Prevention Hotline at 1-(800)-273-TALK or at <u>suicidepreventionlifeline.org</u>. Other resources you may find helpful:

- Ohio Lawyers Assistance Program (OLAP): ohiolap.org.
- Collegiate Recovery Community (CRC): <u>https://swc.osu.edu/services/collegiate-recovery-community/</u>

Basic Needs Security

I encourage any student who faces challenges accessing sufficient food to eat or who lacks a safe and stable place to live, to contact the Assistant Dean for Students for support. You may also notify me if you are comfortable doing so. Other resources you may find helpful:

- Buckeye Food Alliance: buckeyefoodalliance.org/
- Student Advocacy Center: advocacy.osu.edu/

Sexual Misconduct/Relationship Violence

Title IX makes it clear that violence and harassment based on sex and gender are Civil Rights offenses subject to the same kinds of accountability and the same kinds of support applied to offenses against other protected categories (e.g., race). If you or someone you know has been sexually harassed or assaulted, you may find the appropriate resources at <u>http://titleix.osu.edu</u> or by contacting the Ohio State Title IX Coordinator at <u>titleix@osu.edu</u>.

Diversity & Inclusion

The Ohio State University affirms the importance and value of diversity in the student body. Our programs and curricula reflect our multicultural society and global economy and seek to provide opportunities for students to learn more about persons who are different from them. We are committed to maintaining a community that recognizes and values the inherent worth and dignity of every person; fosters sensitivity, understanding, and mutual respect among each member of our community; and encourages each individual to strive to reach his or her own potential. Discrimination against any individual based upon protected status, which is defined as age, color, disability, gender identity or expression, national origin, race, religion, sex, sexual orientation, or veteran status, is prohibited.



Law of Cyberspace

Summer 2023

Online Only

Contact Information:

Prof. Marcel C. Duhamel

216-479-6112 (office) 216-233-4653 (cell) (preferred) He/him/his

Students may reach me at any time using the information above. My preferred method of communication is by email.

Overview

What is the law of the internet? How is it enforced? Is the internet special or exceptional, or is it simply a new variation on long-standing structures? This course will examine the law of the internet – some things old (traditional legal concepts applied to new technological and legal constructs); some things new (government regulation specific to "cyberspace"); and the merging of both old and new legal concepts to govern ever-changing technologies.

Learning Goals

- 1. Students will develop working knowledge of the ways in which traditional US legal concepts do and do not apply to "cyberspace" technologies.
- 2. Students will understand the fundamental provisions of specific technology-related US statutes, including the Communications Decency Act, Stored Communications Act, Wiretap Act, Computer Fraud and Abuse Act, and Digital Millennium Copyright Act.
- 3. Students will demonstrate the ability to analyze and resolve simulated "real world" client problems, including matters involving online privacy, data security, online speech, and eCommerce.
- 4. Students will demonstrate the ability to think creatively in applying traditional legal

concepts (e.g. property, contract, and search-and-seizure rules) to issues concerning a variety of online platforms and communication tools.

5. Students will demonstrate the ability to develop and refine their understanding through discussion and debate.

Required Materials

The casebook for the class is JAMES GRIMMELMANN, INTERNET LAW: CASES AND PROBLEMS. It is available as a PDF download at <u>semaphorepress.com</u> for a suggested price \$30. You will need the 12th Edition (2022). Those who wish to purchase a printed and bound copy can do so at Amazon, where at last report the cost was \$66.60:

<u>https://www.amazon.com/Internet-Law-Problems-James-</u> <u>Grimmelmann/dp/1943689032/ref=sr_1_1?dchild=1&keywords=JAMES+GRIMMELMA</u> <u>NN%2C+INTERNET+LAW%3A+CASES+AND+PROBLEMS&gid=1609787093&sr=8-1</u>

An important note from the author:

"I chose to publish with Semaphore because of their fairer business model. By publishing online, they are able to keep costs much lower: the suggested price is \$30, instead of the \$150 or more you might pay for a comparable casebook from a major publisher. You receive a PDF that you can read on your computer, tablet, or smartphone. You can print out as much, or as little, as you need. If the copy you printed is damaged, you can print the missing pages again, as often as you need.

There is an important bargain here. The success of this business model depends on you. We are trusting you not to buy one copy and share it with all your friends. We are also asking you to pay the suggested price. If you think this bargain is a fair one, please help us help bring casebook prices down by doing your part.

My request: Please pay the suggested price. Reward good behavior."

Also please note: This course is about an actively changing field, and reading assignments may change to reflect current news and developments.

PLEASE READ THE FIRST ASSIGNMENT PRIOR TO THE FIRST CLASS SESSION

We will all have a better experience in the first session if you come prepared, having done the reading.

- o City of Ontario v. Quon, 560 U.S. 746 (2010)
- JG pg 11-14 (Introduction)
- o JG pp. 58-74

Grading criteria

The exam will be an eight-hour, open-book essay exam. I anticipate that the exam will consist of two or three essay questions, each with a strictly enforced word limit.

I will also assign a pair of problems from the casebook as a writing assignment.

Class attendance and participation will also count toward your grade.

Course Policies

Attendance: In conformity with the requirement of College Rule 9.08 and ABA Standard 308, I expect regular class attendance and preparation for class. Having said that, however, I do understand that life comes with conflicts and complications, not all of which are foreseeable. If you run into issues that affect your ability to meet the attendance expectations please contact me to discuss. As is true in the legal practice generally, asking for permission will typically yield better results than will asking for forgiveness.

Preparation: For your benefit and that of your classmates, read the assignments for class and be prepared to discuss them. Better preparation will enhance the value of class sessions. Please note as well that being prepared is one of the key components of a successful legal career, and consequently a skill one is wise to develop while still in school.

As noted above, class attendance is required. Please attend class even if you are not prepared. Class discussion will increase your understanding of the course material and you still may be able to participate.

Participation Tips:

- o Be present
- Spend your class time in class. Avoid spending class time doing other tasks or otherwise not engaging with the class process.
- Have opinions; express them; ask questions.
- Be considerate, compassionate, and respectful toward all others in the class. Don't be afraid to disagree; be respectful when you do.

Academic Misconduct: Academic integrity is essential to maintaining an environment that fosters excellence in teaching, research, and other educational and scholarly activities. Thus, The Ohio State University and the College of Law expect that all students have read and understand the Moritz College of Law Honor Code (<u>https://moritzlaw.osu.edu/registrar/docs/honor_code.pdf</u>), and that all students will complete all academic and scholarly assignments and examinations with fairness and honesty. Students must recognize that failure to follow the rules and guidelines

established in the Honor Code and this syllabus may constitute academic misconduct as defined in Article IV.B of the Honor Code. Examples of academic misconduct include (but are not limited to) plagiarism, collusion (unauthorized collaboration), copying the work of another student, and possession of unauthorized materials during an examination. Ignorance of the Honor Code is never considered an excuse for academic misconduct, so I recommend that you review the Honor Code. If I suspect that a student has committed academic misconduct in this course, I am obligated by College rules to report my suspicions to the College Administration. The sanctions for the misconduct could include a failing grade in this course, suspension or dismissal from the College and University, and a report to the relevant bar authorities. If you have any questions about the above policy or what constitutes academic misconduct in this course, please contact me.

Accommodations:

Moritz is committed to providing an environment that ensures that no individual is discriminated against on the basis of any disability. Students with disabilities (as defined under the Americans with Disabilities Act of 1990) who may need special academic accommodations should notify the Assistant Dean for Students as soon as possible. The dean will work with the student, the Office of Disability Services, and me to coordinate reasonable accommodations for students with documented disabilities. The Office for Disability Services is located in 098 Baker Hall, 113 W. 12th Ave, Columbus, OH 43210; telephone 292-3307, VRS 614-429-1334; http://www.ods.ohio-state.edu/.

Schedule:

Below is a tentative reading schedule. We may vary the speed or order of the readings depending on the needs of the class, and it is highly likely that the specific dates and assignments below will be adapted along the away. As noted above, given the dynamic nature of the subject matter I may also assign additional or varying materials as the semester progresses. The materials we will be studying can be found either in the assigned textbook, through Lexis or Westlaw or, in a pinch, through Google. Copies of any materials not available through these sources will be posted on Carmen.

I. Introduction

- 1. First Thoughts: Adapting the Law to Technology
 - o City of Ontario v. Quon, 560 U.S. 746 (2010)
 - JG pg 11-14 (Introduction)
- 2. Theories and Realties of the Internet
 - a. JG pp. 58-74

II. The Technical Stuff [Brian Donato, guest speaker]

• JG pp. 17-55

III. Jurisdiction

3. JG pp . 68-122

IV. Speech

4. JG pp. 123-194

V. eCommerce

- 5. Amazon, Ebay, et al: An Introduction to eCommerce
 - JG 624-64
 - JG 367-383
 - *Skullcandy, Inc. v. Filter USA, Inc.*, 2019 U.S. Dist. LEXIS 104393 (D. Utah June 21, 2019)

<u>VI. Privacy</u>

6. JG pp. 195-320

VII. Access to Computers

7. JG pp. 325-366

VIII. Platforms

- 29. JG. pp. 547-623
- 30. JG pp 660-682



Comparator Analysis: Cybersecurity, Law, Policy, and Management Certificate

January 2024 | Ohio State Online



Purpose

The purpose of this analysis is to compile the high-level information, including the presentation of that information, prospective learners are seeking most about online programs from comparator/competitor programs at other institutions.



Institutions Analyzed

- Cleveland State University
 - Rationale Regional competitor, parallels to online MSL offering at Ohio State with additional cybersecurity concentration, competitive on price, asynchronous course options, 100% online
- Indiana University Bloomington
 - Rationale similar program to Ohio State (with policy and technical courses), stackable with MS program, top regional competitor, 100% online
- University of Southern California
 - Rationale large national online competitor, multiple program options (standalone, concurrent with another degree), top-ranked law school, 100% online



Cleveland State University



Overview

Program Name: Cybersecurity and Data Privacy Certificate

Offering College: CSU College of Law, CSU College of Business

College of Law Program Page URL: <u>https://www.law.csuohio.edu/academics/curricul</u> um/concentrations/cybersecurityprivacy

College of Business Program Page URL: https://business.csuohio.edu/academics/cyberse curity-and-data-privacy-certificate



Business Page

iio State Onli<mark>ne</mark>

Program Academic Details

Credit Hours Required

The certificate requires 12 credits total.

Program Structure

The certificate requires 6 courses total. The three foundational courses and three electives, one of which must be an experiential learning course or externship.

Course Modality (Sync/Async)

*asynchronous, online sections offered for each of the required courses for non-JD students enrolled in the online MLS or Graduate Certificate

Experiential Learning/Externship

Experiential Learning/Externship:

- In lieu of taking IST 693 or LAW 860, students may opt to have an externship in a legal or corporate setting to satisfy the experiential learning component of this certificate.
- The externship must be approved by the Center for Cybersecurity and Privacy Protection Director or Co-Director.

Affiliations

business dimensions and the legal and regulatory framework. Affiliated with the Center for Cybersecurity and Privacy Protection, housed in the Cleveland-Marshall College of Law, the certificate takes an interdisciplinary approach to address privacy and risk-management concerns.

Core Courses

- L741 Cybersecurity I (3 credits)
- L747 Privacy Law & Management (3 credits)

Elective Courses

ELECTIVES (SELECT 6 OR MORE CREDITS)

Online Law Electives**

- L746 Cybersecurity II (3 credits)
- L690 HIPAA and Privacy (3 credits)
- L701 Corporate Compliance I (3 credits)
- L702 Corporate Compliance II (3 credits)
- L735 Cyberlaw (3 credits)
- L770 Cybersecurity Technical Capstone
- L892 Introduction to American Law***

**only for non-JD students enrolled in the online MLS or Graduate Certificate

***only for non-JD students enrolled in section 81; requires Program Director permission)

LAW ELECTIVES

- L746 Cybersecurity II (3 credits)
- L701 Corporate Compliance I (3 credits)
- L665 Cybercrime (2 or 3 credits)
- L764 Cybersecurity Practicum (3 credits)
- L844 Cybersecurity Risk Assessment and Compliance (3 credits)
- L860 Upper Level Writing (2 or 3 credits) (*topic and advisor must be approved by the Center Director)
- Externship (*placement must be approved by the Center Director)

BUSINESS COLLEGE ELECTIVES

IST 636 Managing Network and Security Risk (3 credits)

IST 656 Advanced Information Security (3 credits)

IST 693 Information Security Risk Assessment (3 credits)

ALTERNATIVE ELECTIVE

A student may seek permission from the Program Director to substitute an alternative technology-related course to satisfy the 3-credit elective requirement.

Admissions and Enrollment

CYBERSECURITY AND DATA PRIVACY CERTIFICATE

Admission Requirements

CSU College of Law's innovative **Cybersecurity and Data Privacy Certificate** takes an integrative approach to education, preparing students to understand the technical and business dimensions of cybersecurity and privacy as well as the legal and regulatory frameworks. Offered by the Center for Cybersecurity and Privacy Protection, this certificate is intended for JD and MLS students.

Admission:

- Although the graduate certificate in Cybersecurity and Data Privacy offers course options from both the College of Business and College of Law, admission to the program is managed by the College of Law.
- Graduate Business students interested in the certificate should contact the College of Law for admissions information.

COMPC	SE E-MAIL	
TO/RECIPIENT		
B.E.RAY@csuohio.edu		
YOUR FULL NAME *		
YOUR E-MAIL *		
SUBJECT *		
MESSAGE *		
Request	for Informatio	on
	Form	
I'm not a robot	reCAPTCHA Proces ¹¹ *rana	

CONTACT US

Program Contact Information

FOR MORE INFORMATION, CONTACT PROFESSOR BRIAN RAY, DIRECTOR, CENTER FOR CYBERSECURITY AND PRIVACY PROTECTION.

RECTOR:	Brian Ray, Professor and Director, Center for Cybersecurity and Privacy Protection
EMAIL:	b.e.ray@csuohio.edu
PHONE:	216-687-2528
W MISSIONS	Please view the College of Law admissions staff <i>here</i> .

THE OHIO STATE UNIVERSITY

Value Propositions

- Opportunity for JD and MLS students to differentiate themselves
- Interdisciplinary
- Experiential Learning Opportunity
- Affiliation with the <u>Center for</u> <u>Cybersecurity and Privacy Protection</u>

Learning Outcomes

We teach law students to understand technology and technical students to understand legal issues in our interdisciplinary cybersecurity and data privacy programs and to work together in real-world situations that require translating between the two.

Students in all of our programs are required to take Cybersecurity I, where they learn the basics of technical security and complete labs using open-source tools to understand common cybersecurity threats. In Cybersecurity II, students apply those concepts by developing technical controls that comply with the data security and privacy laws and regulations that apply to a large public research university. In the required Privacy Law & Management course, students survey the major data privacy and security laws that apply to a large multi-national organization and learn how to develop a comprehensive privacy program to address those overlapping and sometimes conflicting obligations.





Student Support Services/Co-Curricular Features

DIVERSITY, EQUITY AND INCLUSION AT CSULAW

Cleveland State College of Law's commitment to equality runs deep through our history. We were the first law school in Ohio to admit women and one of the first to admit African Americans. Today, CSU|LAW seeks to honor that legacy through dedicated efforts of faculty, administration, staff, and students to listen and evolve to ensure we remain a welcoming law school dedicated to diversifying the profession and a force of justice and equality in the broader community.

JUNE 2020 DEAN'S CALL TO ACTION: NO ROOM FOR SILENCE

DEI Initiative

In June 2020, Dean Fisher issued a **Call to Action** to address racial and social justice and antiracism holistically, including through programming and curricular efforts, and through providing resources and advocacy. To implement the Call to Action, four work groups were formed and engaged in ongoing projects during the 2020-2021 and 2022-2023 academic years:

- School Climate Work Group
- Training and Education Work Group
- Public Action Work Group
- Community Conversations Work Group

Among other projects, the work groups created a series of Community Conversations to engage our community in processing difficult topics. See **No Room for Silence archive page and Racial Justice Task Force archive page**.

Student Support

CULTURE OF BELONGING

Creating a culture of belonging is critical to supporting students to success. In addition to organic connections, students at CSU|LAW find connection through affinity-based student organizations, our College of Law Peer Mentor Program, and programs sponsored by our Office of Student and Career Services.



q

Indiana University - Bloomington



Overview

Program name: Cybersecurity Law and Policy Graduate Certificate

Offering college: Maurer School of Law

Main program webpage URL: https://law.indiana.edu/academics/cyber-certs/law-andpolicy.html

Online Program Page: https://online.iu.edu/degrees/cybersecurity-law-and-policycertificate.html



loomington Netropungti järes Teausanetskinesis 🚳	Indiana University	byen actors & Gentlands Salar Bears & Sear &
3W . Resent JS almount Grallate admission Camet shalers. Name	Cybersecurity Law and F Graduate Certificate	Policy
Terry / Approxima / (Aphroneur) program		
Graduate certificate in cybersecurity law and policy	100% Onliver 12	Science Values for Long Constant Values for Long States and Long Constant Values for Long Science Scie
Society requires individuals with cybersecurity law and policy background to establish		
existing norms and unsafety new challenges.	Cybersecurity Law and Policy Graduate Certificate	
Attrough cybersecurity results are offile thought of an primarily technical, law and policy are officially inspectant skills in their annual Cybertaniarity has and tealwo are only.	Episerce-cartig initial to contractive calify poensi in cyberascartig loss and policy to presentation?	ning, and talined society costs agroung cost for calculate add strategy large and to screen regulators and desire one planters of an and path frameworks in the
beginning to develop and the demand for cyber security professionals continues to receive in the provide and public sectors at the local nullocal, and international levels. A	buckground for hear establish the properties got construction over challenges.	to exercise to require legisly for any control including is discussing satisfy service of
Iree examples. Builtrate the breadth and need for individuals with a law and policy background in cybersecurity. Consumer make are created by the Internet of Things.	The for Danism File electric Control on Controls in Controls in the Control of Control of Control of Controls (Control of Control o	serby Law and Policy is using ety (accelered 3) a rown from an invariant because of its shows, and computer sciences is a statistic in the program, yes analy 12 before and state is concerned with the statistic of the statistic in the statistic of the statistic of the statistic science of the statistic of the st
Safety risks are created by self-driving whicles. Democratic risks are created by various Invests to elections. National security risks are created by threats to technology ted to	importability for spheroimarty. Her regulation You regime contents of spheroimarthy law in oth	ry privery and paind chine, and other bank available for them. We parts of the ways and their likely impact on US institutions. The wark to assess
ritical infrastructure	 (plus second) card, segliarline, and added attention and attention input or policy analytic through encoded and they may prove that 	ensors a barre of their receiver or ordinations and indexiduates and effectiveness. - relight class track advects was indexinguine, applications products, and any costs in terms of - Their indexinguine and existing two. You also have to cost of any the backet context in
Is address these max, society requires not only individuals with technological expertise, but also individuals with cybersecurity law and policy background to help establish the	which of the time of the product of all of the range	was that an deep to be manualed by efforts to address systems at the designs, including it associates, efforted community and tableed learning
per upper representes for responding to the ways that sectorality is an apply a storage pointing rest, and creating new challenges. There is a growing need for activations with formal	Galaryana Bulky generate Salaryana Bulky generate	
generation of the set	 Internation paramity analysis Computer and address statistics reported international Vision of the parameters 	-
out the certificate	Prese generated Prese product Prese product Contracted Contracted	
Mazer School of Law and Industa University Bioprington are uniquely placed to are Thread theorem to be used of date and forced constrainty in advantation and research	Cartificate Regularments	
beneducity and information privacy. Recognized by the federal government as a null action of an observe transforms in Coher Talance Enter that (CAE-CTE) and	To easy the Graduatic Centitude in Cylinececca Sequencements are inciden down as follow:	rhy Law and Parking, you music completion at lives 12 could income
enal Center of Academic Excellence in Cyber Defense Research (CAE 49), 10's enacurity and efformation privacy programs are distinguished by their	 Cylineraeut er by law und parkity men experience + Cylineraeut (Ky law und parkity erective source) 	3 12 small feart) n (pr. emind in 10.00 12 small fearly
endisciplinary approach, including integration of law, business, and computer science	"Courses for the contribute program on other secondary	allock artise and an ampla. Places that the cartest scarae listings for writes
FO/bersecurity Law and Policy Certificate can be warred on campus in Bloomington online from anywhere in the world. The Maxeer School of Law will award a graduate		
Fronte to students who complete at leads 12 coefficients in courses specified below in marketings, marketing, marketing below averaged 31.0.4.8 coefficients and the student during the application of the 30 coefficients required for a <u>Minder's of</u> marketing and the Statistication of the statistication of the statistication of the statistication of the statistication of the statistication of the statistication of the statistication of the statistication of the statistication of the statistication of th	 METE, Prove descent to public the Edition of engineerism. Comparison of the certificativity 	It is of photons only that Management I have undifficient outwark your, builty to one vispose operations wit put when all the unit in the graduals property.
as required for certificate	Admissions To be accepted to this program, yo	o must have:
press.	1. Alian tenter 5 angewe Still 17 Tricipenginan is authorited even	et and subject to the regulatory simplicies are may reset that etc. Non all 10 etc.
ust take one of the following two core courses (and may take both): security Law ((3 or)	To apply to this program, complete - Tamatian	an ordine application that includes:
recently Law (Ork)	Personal cluberard Security	
ta technology background must take:	Courses	
ag and Tachnology Boot Earry (3 or) in the Tohool of Information. d:Engineering	Core - Hfmduction to US Law - 1 Cr	edt +
or legal experiences, whereas next concurrently envirolled in the 2D least two and to at RPG-1 interest relation to a residue of RPG-1 interest relation to a resi	Core - CSCI-K541 - Computing and	Technology Boat Camp - 3 Credits +
	Gare	
ct truth a list of designated courses to satisfy the balance of the 32 of for the certificate. These courses include:	LAN \$127 Internation 5	acutyLas 3 Death
theory Law (Constitutional Privacy Image (Box)	UN 6731-08-0040 Coloreducts	Lan - Oh - Syltemetra Ny Law and Tology
Trainciane II. Privace Resolution (3 or) traine (2 or)	Decise	0.65
Privacy and Texastic Management Practician (Tex.)	(50) 4342 Submatria.easte	an-at Cybernecarly 3 Deaths
nertran response Lawe. Data: Lawe and Policy (2 or)	BARD F180 IT for biologeneet	i item
sion to the certificate program. JD students must apply to and be	Line 0.000 Health Princip Law	20em
a of an E2 research cantae with cybernesseity or information no of tocus. These include the long established <u>Center for Applied</u>	UN 6759 eterratio Pracy	(air) Carethiliteal Prezy Issain Scheeth
The new Ostrom Workshop Programmon Oxtensecturity and aw School students are not required to affiliate with a	Link 8.128 Internation Privacy	Las il Anuny Regulation 3 Dantis
	UNIT 1711 Sector is a resident	ar Property Case Data Case and Policy & Election
f of Law 2D students:	Toticions description with our Search So Tuiltion & Fees	nemen er sammer förstam fred.
tion application (2). Even submit it to Prof. Joe Tomain at:	Cost for Indiana Residents - Per Credit Hour	Cost for Out of State Residents - The Credit Nour
	Summer Matternet Strength Houses	 Farlow EDB600 3 Condit Nears
Intersity Graduate School admissions page. From the drop- sementer in which you would like to start your studies.	Same Setting	+ Tailon (MAD III)
ton to be taken to the indiana University Graduate CAS sign in for sign in to your existing account.	The angular is required in the annual that requirements and a second process with the description of the transport of the second secon	ette, furtue cancelater a "Cord of Attendance" for the program harmonic barrows and sciences
w" into the search bar to find the Cybersecurity Law and Policy "into Cick the observices both and the certification."	 Second way was changed on an original full to Second way our this are party services (SA) and this builts are suggests through the second way. 	Sea number of all to fight the state of a single sensible. You advantation to the full ACCS- term numbers of all to fight that the state of a single sensible. You advantation to human present separate will vary based on
 A state of the sta	 The standard of could loads proclaim - Workford procise an industry reaction + You'r among choices 	
App "tail to trish building your application.	* Your tool Public Your coult of effortients your differ from these to	nievin.
attrivuon in the Fall sensesher. Apply by December 1 for admission in	ful line likeling	Part Section (Section
lease contact.	Deept Dashe	Deep Coute.
	Tradition & Manufacture y France Inclusion Transform	Tables & Manufating Page Instants Transfords
carly and inference on Privacy care Programs as indexes (inservice)	have per conditions with which also as	las proceditivas vals interfacione Natural (201
	Seis per coditi faur min Advotatione	See per credition one infectione
	Mentilats.	sated Date.
spected to demonstrate.	foor E-marchine - Land all all	Instances Their
Indexia and state laws and regulations and major justicial opinions sarity.	Robot & Degree 1010	from A Suppose. XXX
5. Noteral and state regulators with responsibility for statury powers and jurisdiction, and other tools available to	Transportatione 32458 Annuard Experiment. 34523	Tomportan kirili Peruna Lipenan, kirili
models of subservery by law in other parts of the parts?		
end impact on U.S. institutions:	Pyra read like prove in	elained experience of respectation, primate uses for 1 Subtract and Free Damagnation
es of internation about cybersecurity issues. Inchrologies. The ability to assess their relevance, accuracy, and reliability:		Bollands & Statement
ensecurity laws, regulations, and judicial decision in terms of their expact on institutions and individuals, their efficiency.	What's it like to be an IU Onlin	e Student?
and offher legal or policy taskets they regeld ratio: technologies, applications, products, and services in terms of	Earth an IV education from whereas Whee you ereal man G Orice program, you't same foods whe hard on or	neelliinen, taagiite Se
tey-trady present and their lawfulness under existing law, and runder context in which cybersecurity issues occur and other	 the fire fire affectable way is get the 10 will putting your time or same vertical. 	and the year deserve without
be implicated by efforts to address cyberaecuity challenges, many, threadens of expression and association, efficient	Get the support you need to succes	ed .
al security	As a student of air to choice program, positivities and seek level them your patholics and peers, to evidence and	we the appart and y to engage with. Such as you would be a company
slacking tambardy with U.S. law will be expected to demonstrate:	fracti also (pare access to a variety of academic (excast call or when you year) actificant access	cand other nagged services that tarols, Rochs an important part
Ing or the basic structure of U.S. law and the U.S. legal system with information technologies will be expected to	of the transmission of part were definition to en- processed by these regions defining responses	suring produce the resources
W	Reap the rewards for decades to on to matter what hill provide a set of more an	une and the set of prove pair
nding of computers, networks, and mobile devices, and how they	chances of sample providence or payments. The Table same party table with here payments.	on harmonic Onlin
g of "big data" analytics and algorithms: and or of sufferentiation taxis.	Adams whether practice constrainty to compared on held-or-constraints and particles.	anarcas agene in your surrent
	Take the first step toward a more n	ewording future
f 8 a ++	Pergnant Mare Information	
Alana Telensoly Manus Scheol et Lae Date Hell 22 South Holena Aleman	APPLYNON	
Barrangha, N. (200) Caraanar of analon (201) og and de invarni		I saw the same same same

11

line Program

Page

U Indiana

A myre Gostado depo Courses Arazo of basis Gotal experior Public internet Experiental est Tamby office pr Cyberneurshy grageres Cyberneurshy orthoge

Main Program

Page

Program Academic Details



NOTE: If you choose to pursue the IU Online MS in Cybersecurity Risk Management, these certificate courses may apply to your degree requirements. Completion of the certificate program does not guarantee admission to the graduate program.

	Courses	
Core		
LAW-B 587	Information Security Law	3 Credits
LAW-B 738OR BUKI T 578)- Cybersecurity LawOR Cybersecurity Law and Policy	3 Credits
Elective		
CSCI-A 542	Technical Foundations of Cybersecurity	3 Credits
BUKD-T 560	IT Risk Management	3 Credits
LAW-B 536	Health Privacy Law	2 Credits
LAW-B 655	Information Privacy and Security Management Practicum	3 Credits
LAW-B 708	Information Privacy Law I Constitutional Privacy Issues	3 Credits
LAW-B 728	Information Privacy Law II Privacy Regulation	3 Credits
LAW-L 730	Seminar in Intellectual Property Law: Data Law and Policy	3 Credits

Core and Elective

Program Academic Details

Total Cost Estimate

Full time Students	Part time Students	
Direct Costs:	Direct Costs:	
Tuition & Mandatory Fees	Tuition & Mandatory Fees	
Indiana Residents	Indiana Residents	
See per credit hour rate listed above	See per credit hour rate listed above	
Non-residents	Non-residents	
See per credit hour rate listed above	See per credit hour rate listed above	
Indirect Costs:	Indirect Costs:	
Food & Housing \$15,456	Food & Housing \$15,456	
Books & Supplies \$830	Books & Supplies \$302	
Transportation \$2958	Transportation \$2958	
Personal Expenses \$4078	Personal Expenses \$4078	

Cost Per Credit Hour

Per Credit Hour

Cost for Indiana Residents

- Tuition: \$1369.00
- 3 Credit Hours
- Tuition: \$4107.00

Note: Additional fees will apply. -This program is ineligible for financial aid.

Financial Aid

This program is ineligible for financial aid.

IU Tuition & Fee Calculator

• Per Credit Hour

Cost for Out of State Residents

- Tuition: \$1369.00
- 3 Credit Hours

Tuition: \$4107.00

Accreditation

on cybersecurity and information privacy. Recognized by the federal government as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) and National Center of Academic Excellence in Cyber Defense Research (CAE-R), IU's

Affiliations

Center affiliation

As a condition of admission to the certificate program, JD students must apply to and be accepted as a JD affiliate of an IU research center with cybersecurity or information privacy as a principal area of focus. These include the long-established <u>Center for Applied</u> <u>Cybersecurity Research</u> and the new <u>Ostrom Workshop Program on Cybersecurity and</u> <u>Internet Governance</u>. Non-Law School students are not required to affiliate with a Research Center.

Admissions and Enrollment

Program Start Dates

Apply by July 1 for admission in the Fall semester. Apply by December 1 for admission in the Spring semester.

Admission Requirements To be accepted to this program, you must have:

1. A bachelor's degree

Application Requirements To apply to this program,

- Transcripts
- Personal statement
- Resume
- At least one reference



Apply by July 1 for admission in the Fall semester.	. Apply by December 1 for admiss
the Spring semester.	
FireForm Information	t for n Forms
Home / IU Online / General Information Request	
Request Information from IU Online	
First Name (* required)	
Last Name (* required)	Call
Email (* required)	
Phone	Prog
Primary Zip/Postal Code (* required)	Joseph A. Tomain Senior Lecturer in La Director of Cybersec Maurer School of Lav
Choose an option	(812) 855-0466 itomain@indiana.edu

Application Deadlines



Ohio State Online

Value Propositions

- Credit toward a master's degree
- Interdisciplinary approach
- Preparation for in-demand careers
- Responsive to students
- Flexible, affordable

Main Value Proposition

The IU Online Graduate Certificate in Cybersecurity Law and Policy is uniquely positioned to answer these demands because of its interdisciplinary approach, integrating law, business, and computer science. As a student in the program, you study US federal and state laws and regulations and major judicial opinions concerning cybersecurity, as well as the major US federal and state regulators with responsibility for cybersecurity, their regulatory powers and jurisdiction, and other tools available to them.

Program Differentiators

Earn an IU education from wherever you are

When you enroll in an IU Online program, you take IU classes, taught by the same faculty who teach on our campuses.

It's the flexible, affordable way to get the IU education you deserve without putting your life—or career—on hold.

Learning Outcomes

All students will be expected to demonstrate:

- Familiarity with U.S. federal and state laws and regulations and major judicial opinions concerning cybersecurity;
- Familiarity with major U.S. federal and state regulators with responsibility for cybersecurity, their regulatory powers and jurisdiction, and other tools available to them;
- Familiarity with major models of cybersecurity law in other parts of the world, and specifically their likely impact on U.S. institutions;
- Familiarity with sources of information about cybersecurity issues, technologies, threats, and law, and the ability to assess their relevance, accuracy, and reliability;
- The ability to assess cybersecurity laws, regulations, and judicial decisions in terms of their likely effectiveness, their impact on institutions and individuals, their efficiency, their cost-effectiveness, and other legal or policy issues they might raise;
- The ability to assess new technologies, applications, products, and services in terms of the cybersecurity issues they may present and their lawfulness under existing law; and
- An understanding of the broader context in which cybersecurity issues occur and other values that are likely to be implicated by efforts to address cybersecurity challenges, including information privacy, freedom of expression and association, efficient commerce, and national security.

Career Outcomes

- Cybersecurity policy specialist
- Security management specialist
- Information security analyst
- Computer and information systems manager
- Vulnerability assessor
- Privacy specialist
- IT specialist
- Cybersecurity specialist

The Ohio State University

Student Support Services/Co-Curricular Features

Support resources

What's it like to be an IU Online Student?

Get the support you need to succeed

As a student in an IU Online program, you'll have the opportunity to engage with and seek help from your professors and peers, just as you would in a campusbased program.

You'll also have access to a variety of academic and other support services that you can call on when you need additional assistance. You're an important part of the IU community and we're dedicated to ensuring you have the resources you need to thrive in your online program.

Responsive to Students



IU's response times beat other schools. I was happy with the application and admissions process, and with the follow-up I received when I called for more information.

University of Southern California





Overview

Program name: Privacy and Cybersecurity Certificate

Offering college: USC Gould School of Law

Main program webpage URL: https://gould.usc.edu/academics/certificates/privacylaw/standalone/

Online Program Page: https://online.usc.edu/programs/privacy-lawcybersecurity-certificate/



> an Uproming Events



THE OHIO STATE UNIVERSITY

Main Program Page

Program Academic Details

USC Gould's online Privacy Law and Cybersecurity certificate provides
you with the fundamental knowledge to understand the necessary legal
parameters of our increasingly interconnected world.

Students will have the opportunity to explore legal frameworks concerning information privacy in the U.S. and common legal issues and emerging laws in privacy and cybersecurity. The program prepares graduates for leading roles in protecting business and individual data with essential legal background, policies and best practices that preserve digital integrity today.

The online Privacy Law and Cybersecurity certificate is ideal for those who want to learn more about the latest privacy and security-focused laws and how it affects such fields as:

- Business and corporations
- Regulations in digital and data-sharing industries

The Ohio State University

- Technology and software development
- Individual and organizational policy
- Lawyers and law firms

Information Management & Risk (2 units)

Course Descriptions

This class will teach students best practices for overseeing the development, implementation, maintenance and adherence to current privacy laws and regulations. Students will learn how to manage and mitigate risk associated with the acquiring, storage/retention, use, sharing and disposing of data. Upon completion of the course, students will be able to identify privacy and data protection issues, communicate effectively about privacy and data protection issues, and offer solutions to relevant stakeholders such as customers, end users, suppliers, vendors, regulatory authorities, and others.

Information Privacy Law (2 units)

This course will examine the legal and policy issues pertaining to information privacy in the United States. The course will address the privacy issues facing both the public and private sectors, particularly in response to the growing emergence of cybercrimes and cybersecurity issues. Topics will include: the concept of privacy, privacy in the information age particularly in the current cyber threat environment, privacy and the media, consumer data, employment issues, government access to information and the Fourth Amendment, national security issues, and international privacy issues.

Program Snapshot

Academic Unit

USC Gould School of Law

Department or Academic Program

Privacy Law and Cybersecurity

Admission Requirements

- Bachelor's degree in any field
- Official transcripts from all universities attended
- Personal statement
- Resume
- LSAT: Not Required
- TOEFL or IELTS score, if international applicant

Program Length

Students can complete the program in 12 months.

.....

Practicum Requirements

Program is completely online.

Program Website

For additional details and to learn more, visit the program's website.

LEARN MORE

Credit Hours Required and Curriculum Overview

Earning the online Privacy Law and Cybersecurity certificate requires successful completion of 12 credit units, including the following mandatory courses.

Cybersecurity & Cyber Crimes (2 units)

Curriculum

Global Regulatory Compliance (2 units)

Information Management & Risk (2 units)

Information Privacy Law (2 units)

- Regulatory Compliance (2 units)
- Patient Privacy Law (2 units)

.

Learning Outcomes

Learning Outcomes

Through the online Privacy Law and Cybersecurity certificate, you will:

- Learn advanced legal terminology specific to data privacy and cybersecurity laws
- Obtain practical knowledge of the legal profession
- Strengthen your critical thinking skills
- Review and draft agreements, policies and other documents to effectively mitigate and manage risks
- Research cybersecurity laws and privacy issues affecting individual and corporate entities
- Review cybersecurity-related content for compliance with federal and state regulations

Program Academic Details

Total Cost of Attendance

Tuition for the online standalone certificate for 2023-2024 academic year is \$35,472, plus university fees, as described below.

Tuition	\$2,956 per unit	
Graduate Programming Fee	\$20 per semester	
Norman Topping Student Aid Fund	\$11 per semester	
Tuition Refund Insurance (Optional)	\$35 per semester	
Student Health Incurance (Waiyable)*	Fall 2023: \$1,754	
Student Health Insurance (waivable)"	Spring 2024 and Summer 2024: \$3,388	
*Student health insurance can be waived if proof of coverage is provided by the deadline set by USC Student Health.		

Textbooks and other course materials average \$500 per semester.

Scholarships

Scholarships

You will receive automatic consideration for USC Gould's merit-based scholarships. Scholarship offers are released at the time of admission.

Paying for your Degree

USC's Office of Student Financial Services Ø offers numerous payment options, including an interest-free USC Payment Plan for tuition and fees paid in monthly installments.

Federal Loans

U.S. citizens and permanent residents who wish to pay for school through loans from the U.S. government must complete the Free Application for Federal Student Aid # (FAFSA). The FAFSA can be completed as early as October 1 of the year prior to the year in which you intend to enroll, and should be completed as early as possible. USC's school code is 001328.

After you have successfully completed the FAFSA, and have been admitted, you will receive an electronic notification from USC Gould's Office Financial Aid office with additional information and instructions on the federal loan application process. For additional details about the student loan options available to graduate students, please click here #.

Private Loans

USC's Office of Financial Aid offers information about private educational loans #.

Corporate Billing

USC students who are sponsored by a company; a local, state, federal, or international governmental agency; or branch of the U.S. military may be eligible to have all or a portion of their bills sent directly to the sponsor. Payment by the sponsor is due upon receipt of the bill. The charges paid by the sponsor can vary - some will pay for tuition and mandatory fees, others will also pay for parking, housing, dining, or other charges. The student is responsible for paying any charges not authorized by the agency. For more information on how to arrange for corporate billing visit the USC Agency Billing # office.

Employer Reimbursement

USC students who receive tuition reimbursement from their employer have the opportunity to defer up to 75% of their tuition payment until the end of the semester. Students whose employers reimburse at the end of each semester rather than paying for tuition upfront should visit USC's Student Financial Services' website #.

Veteran Benefits

USC students who are active duty military personnel and veterans may qualify for education benefits through various Veteran Affairs (VA) and State programs. Please visit VA Resource Center # for details on available programs.

Follow this link to the U.S. Department of Veterans Administration # web page on education and training benefits.

Follow this link to the California Department of Veterans Affairs # web page on education benefits

Financial Aid



Admissions and Enrollment

Program Start Dates and App Deadlines

We offer three starts throughout the year in fall, spring and summer. Below are the upcoming start dates and application deadlines:

Program Start Date	First Day of Classes	Applications Open	Priority Application Deadline	Application Deadline
Spring 2024	January 10, 2024	August 2, 2023	October 11, 2023	November 8, 2023
Summer 2024	May 8, 2024	November 29, 2024	February 21, 2024	March 20, 2024
Fall 2024	September 4, 2024	January 17, 2024	June 19, 2024	July 17, 2024
We recommend applying by the priority application deadline for scholarship consideration.				



Application Requirements

3. Resume/Curriculum Vitae (CV)

4. Transcripts

5. English Proficiency - International Applicants

Admission Requirements

• Bachelor's degree in any field

Admission

Requirements

Official transcripts from all

universities attended

- Personal statementResume
- LSAT: Not Required
- TOEFL or IELTS score, if
- international applicant

Program Contact

Program Contact

USC Gould School of Law Graduate and International Programs (213) 821-5916 msl@law.usc.edu



Request for Information Form

Decision Timeline

Interested? Learn more.



CLICK HERE TO APPLY ONLINE

Decisions

The Admissions Committee will only review your application once all transcripts and supporting documents are received by the application deadlines shared above. You will receive a confirmation email when your application has been complete. Admissions decisions are normally released by email within two to four weeks of application confirmation. If you are admitted and decide to enroll, a commitment deposit will be required to reserve your seat.

Prior Experience

Prior experience in law is not required

Testing Requirements

You are not required to take the LSAT exam; however international applicants are required to take the TOEFL or IELTS exam.

The Ohio State University

Value Propositions

- Stackable into LLM and MSL programs
- Top-ranked law school
- Learn alongside MSL and LLM students
- Flexibility for working professionals
- Dynamic and engaging online learning environments

Main Value Proposition

The online Privacy Law and Cybersecurity certificate - taken independently or concurrently with our online Master of Laws (LLM) or online Master of Studies in Law (MSL) - will provide you with a competitive edge in the emerging field of data privacy and security, whether you are a recent university graduate or an established professional.

Career Outcomes

- Chief Privacy Counsel
- Corporate Counsel
- Data Privacy Officer
- Director, Information Security and Compliance
- Product Counsel
- Vice President, Information Technology

Learning Outcomes

Through the online Privacy Law and Cybersecurity certificate, you will:

- Learn advanced legal terminology specific to data privacy and cybersecurity laws
- Obtain practical knowledge of the legal profession
- Strengthen your critical thinking skills
- Review and draft agreements, policies and other documents to effectively mitigate and manage risks
- Research cybersecurity laws and privacy issues affecting individual and corporate entities
- Review cybersecurity-related content for compliance with federal and state regulations

Why Choose the Privacy Law and Cybersecurity Certificate at USC Gould?

Follow G&IP on Instagram

Other Multimedia



You will learn alongside our online LLM and online MSL students in a dynamic and engaging virtual classroom. Our innovative data privacy degree program fosters interaction among students and our outstanding law faculty, who design courses to ensure you gain a foundation in legal and business issues in the data privacy and cybersecurity field. The online curriculum provides a convenient, flexible way to pursue this advanced training, while meeting the demands of your profession.

Privacy Law and Cybersecurity Certificate - Online

USC Gould School of Law

Main Imagery





Student Support Services/Co-Curricular Features



Ohio State Online

Evidence-Based Effective Practices

Best Practices to Maximize Student Interest and Accommodate the Working Professional

- **Rolling admissions**: Ensure that the program has a rolling admissions process, whereby applications are evaluated as they are received, and students are notified in a timely manner about the status of their application
- **7-week courses**: Optimal for working professionals, as they provide the flexibility needed to accommodate their busy lives
- **6 start dates/year**: Multiple start dates allow working professional students the opportunity to enroll in programs that meet their needs when they want those needs met

Observations & Considerations

- Comparable certificate programs offer 100% stackable credits into related master's programs. Certificates can be earned as standalone or embedded certificates in related master's programs, offering a differentiating factor for both the certificate and the associated degree programs. The college should consider how this certificate could be stacked into related degree programs outside of the proposed Master of Cybersecurity program.
- Consider how this graduate certificate may align with the Ohio State Master in the Study of Law's concentrations and proposed online certificates. Creating pathways into currently offered Master's programs through "stackable" credentials appeals to working professional students.
- Consider how this graduate certificate may contribute to an additional MPAL specialization or MPA "Stream." Indiana University – Bloomington, offers a <u>dual degree in Public Administration</u> (MPA) and Cybersecurity Risk Management



Observations & Considerations

- Consider how this program could align with industry-recognized credentials, such as the credentials issued by the <u>International Association of Privacy Professionals</u>, to help prepare students for further advancement in their field. Nationally, <u>over 6,000 jobs</u> in the past year mention at least one of these credentials in their job posting.
- Comparable programs offer pre-requisite courses in U.S. law and computing/technology for professionals who have no background in these fields. Students with backgrounds in these fields can bypass these courses to expedite the time to completion. Consider how this degree could be flexible to audiences with various professional experiences in law, cybersecurity, or policy.

Cybersecurity Programs in Ohio

Last Update: 5.20.2024

Air Force Institute of Technology – Graduate School of Engineering & Management

Master of Science in Cyber Operations¹

Dr. Robert Mills, PhD. | Professor | Robert.mills@afit.edu | 937-255-6565 x4527 Dr. Adedeji B. Badiru | Dean, Graduate School of Engineering & Management | 937-255-3636 ext. 4799

American National University

- Bachelor of Science in Cyber Security (Online)²
- Master of Science in Cyber Security (Online)³

James Webb | Program Director, Information Technology

Antioch University Midwest

• Bachelor of Arts in Liberal Studies, Information Technology—Cyber Security Concentration⁴ Hays Moulton | Chair, Undergraduate Programs | <u>hmoulton@antioch.edu</u>

Baldwin Wallace University

• Bachelor's Degree, Cybersecurity Analyst Major⁵

Dr. Andrew Watkins, PhD. | Chair and Associate Professor, Computer Science and Engineering Department | anwatkin@bw.edu | 440-826-2396

Belmont College

- Associate of Information Technology, Cyber Security & Computer Forensics⁶
- Cyber Security Certificate⁷

David McLeod | Temporary Full-Time Professor, Information Technology | <u>dmcleod@belmontcollege.edu</u> | (740)695-9500 Ext. 1198

C-TEC

• Cyber Security Program Lauren Massie | Director of Adult Education | <u>lmassie@c-tec.edu</u> | 740-364-2832

Cedarville University

- Bachelor of Science in Computer Science, Cyber Operations Specialization⁸
- Bachelor of Science in Cyber Operations⁹
- Graduate Business Certificate in Cybersecurity Management (online)¹⁰
- MBA in Cybersecurity Management (online)¹¹

¹ <u>https://www.afit.edu/EN/programs.cfm?a=view&D=13</u>

² <u>https://an.edu/programs/bachelors-degrees/cybersecurity-bachelors/</u>

³ https://an.edu/programs/masters/master-of-science-cybersecurity/

⁴ <u>https://www.antioch.edu/midwest/degrees-programs/undergraduate-studies/liberal-studies-ba/information-technology/</u>

⁵ <u>https://www.bw.edu/academics/undergraduate/cybersecurity-analyst/</u>

⁶ http://www.belmontcollege.edu/current-students/programs-of-study/cyber-security-computer-forensics/

⁷ <u>http://www.belmontcollege.edu/current-students/programs-of-study/cyber-security/</u>

⁸ <u>https://www.cedarville.edu/academic-programs/computer-science</u>

⁹ <u>https://www.cedarville.edu/academic-programs/cyber-operations</u>

¹⁰ https://www.cedarville.edu/academic-programs/cybersecurity-management-graduate-certificate

¹¹ https://www.cedarville.edu/academic-programs/mba-cybersecurity

Dr. Bob Chasnov | Dean, School of Engineering and Computer Science | <u>chasnovr@cedarville.edu</u> | 937-766-7683

Dr. Seth Hamman, PhD. | Director, Associate Professor Cyber Operations and Computer Science | 937-766-7686

Dr. Jeffrey Haymond, PhD. | Dean School of Business Administration; Professor of Economics | 937-766-4442

Clark State Community College

- Associate of CyberSecurity/Information Assurance Technology¹²
- Cyber Security Short-Term Technical Certificate¹³
- Agreement with Wright State to major in Cyber Security (Clark State Wright State)¹⁴

Dr. Aimee Belanger-Haas, PhD. | Dean of Business and Applied Tech | 937-328-6038

Columbus State Community College

- Associate of Applied Science in Computer Science Cyber Security¹⁵
- IT Security Stackable Certificate¹⁶

David Nowak, MBA | Interim Chairperson, Information Systems Technology | <u>dnowak1@cscc.edu</u> | 614-287-2554

Cuyahoga Community College

- Cyber Security Analytics Certificate¹⁷
- Network Administration and Support¹⁸
- Associate of Applied Business in Cybersecurity¹⁹
- Associate of Applies Business in Information Technology Programming and Development, with a Concentration in Quality Assurance²⁰
- Cybersecurity Post Degree Professional Certificate²¹

Dr. Keith Lyons, PhD. | Professor, IT Center of Excellence | keith.lyons@tri-c.edu

Office of Information Technology Training | computertraining@tri-c.edu

Defiance College

- Bachelor of Science in Cyber-Forensics²²
- Minor in Cybersecurity²³

Timothy Wedge, M.A. | Associate Professor, Cyber-Forensics| twedge@defiance.edu

Eastland-Fairfield Career & Technical Schools

- ¹⁴ <u>https://www.wright.edu/sites/www.wright.edu/files/page/attachments/Clark_Computer Science_BA_Cyber.pdf</u>
- ¹⁵ https://catalog.cscc.edu/programs/Computer Science Cybersecurity Major AASI
- ¹⁶ <u>https://catalog.cscc.edu/programs/IT%20Security%20Stackable%20Certificate</u>

- ²⁰ <u>https://www.tri-c.edu/programs/information-technology/programming-and-development/programming-development-at-tri-c.html</u>
- ²¹ <u>https://www.tri-c.edu/programs/information-technology/cyber-security/cybersecurity-post-degree-professional-certificate.html</u>

¹² https://www.clarkstate.edu/academics/degrees-and-certificates/computer-and-information-technology/cybersecurity-information-assurance-technology/

¹³ https://www.clarkstate.edu/academics/degrees-and-certificates/computer-and-information-technology/cybersecurity-short-term-technical-certificate/

¹⁷ https://www.tri-c.edu/programs/information-technology/cyber-security/cyber-security-analytics-certificate.html

¹⁸ http://www.tri-c.edu/programs/information-technology/professional-development/cyber-security/network-administration-andsupport.html

¹⁹ https://www.tri-c.edu/programs/information-technology/cyber-security/cybersecurity-associate-of-applied-business.html

²² <u>http://www.defiance.edu/academics/sm/cyber-forensics/index.html</u>

²³ <u>http://www.defiance.edu/academics/sm/cybersecurity-minor.html</u>
Network and Cybersecurity Specialist²⁴ •

Angela Ward | Director, Workforce Development | AWard@efcts.us | 614-836-4541

Edison State Community College

- Associate of Applied Business in Cybersecurity²⁵
- Computer Information Systems Networking & Computer Information Systems Systems Administration (Less-Than-One-Year Technical Certificate)²⁶

Rich Valerio | Director, Cybersecurity Program | rvalerio@edisonohio.edu | 937-778-7825

Franklin University

- Associate of Science in Cybersecurity²⁷
- Bachelor of Science in Cyber Security (online)²⁸ •
- Master of Science in Cybersecurity²⁹

Dr. Todd Whittaker, PhD. | Program Chair, Information Technology and Cybersecurity | Todd.whittaker@franklin.edu

Hocking College

Associate of Cybersecurity and Network Systems³⁰

Jacob Bookman | Network Engineering & Information Technology | bookmanj22847@hocking.edu

Kent State University

- Computer Forensics and Security Minor³¹
- Bachelor of Science in Computer Science with a Concentration in Information Security³²
- Bachelor of Science in Information Technology with a Concentration in Cybersecurity and • Forensics³³
- Master of Science in Computer Science with a Concentration in Computer Security³⁴ •
- Computer Forensics and Information Security Undergraduate Certificate³⁵

Dr. Javed Khan, PhD. | Chair, Department of Computer Science | javed@kent.edu | 330-672-9055

Lakeland Community College

- Associate of Applied Business with a Concentration in Cybersecurity³⁶
- IT Professional Certificate with Cybersecurity Focus³⁷

Jennifer Crissman | Professor/Department Chair, Information Technology and Computer Science | jcrissman@lakelandcc.edu | 440-525-7267

²⁴ http://www.eastlandfairfield.com/ProgramsandCourses.aspx

²⁵ http://catalog.edisonohio.edu/preview_program.php?catoid=25&poid=5279&returnto=3234

²⁶ http://catalog.edisonohio.edu/preview_program.php?catoid=26&poid=5795&returnto=3630

²⁷ <u>https://www.franklin.edu/degrees/associates/cybersecurity</u>

²⁸ <u>https://www.franklin.edu/degrees/bachelors/cybersecurity</u>

 ²⁹ https://www.franklin.edu/degrees/masters/cybersecurity
³⁰ https://www.hocking.edu/cyber-security-and-network-systems

³¹ http://catalog.kent.edu/colleges/ap/computer-forensics-security-minor/

³² http://catalog.kent.edu/colleges/as/cs/computer-science-bs/

³³ http://catalog.kent.edu/colleges/ap/information-technology-b

³⁴ http://catalog.kent.edu/colleges/as/cs/computer-science-ms/

³⁵ <u>http://catalog.kent.edu/colleges/ap/computer-forensics-information-security-undergraduate-certificate/</u>

³⁶ https://www.lakelandcc.edu/web/about/cybersecurity

³⁷ https://www.lakelandcc.edu/web/about/cybersecurity

Lorain County Community College

- Associate of Applied Science in Computer Engineering Technology- Computer and Digital Forensics Major³⁸
- Associate of Applied Science in Cyber and Information Security³⁹
- Computer Information Systems-Information Security for Business Short-Term Certificate⁴⁰
- Computer Information Systems –Network Security Foundations Short-Term Certificate⁴¹
- Computer & Digital Forensics One Year Certificate⁴²

Kelly A. Zelesnik | Dean, Division of Engineer, Business, and Information Technologies | jzelesni@lorainccc.edu | 440-366-7028

Marion Technical College

- Associate of Computer Information Technology with a Concentration in Cyber Security⁴³
- Associate of Computer Information Technology with a Networking Option⁴⁴
- Computer Information Technology Networking Certificate⁴⁵
- Cyber Security Analyst One-year Technical Certificate⁴⁶

Deb Stark | Dean, Technical and Professional Programs | starkd@mtc.edu | 740-386-4165

Malone University

• Bachelor of Arts in Cybersecurity⁴⁷

Dr. James F. Glasgow | Professor of Computer Science | jglasgow@malone.edu

Miami University

• Bachelor of Science in Cybersecurity⁴⁸

Scott Campbell | Senior Director of Technology | campbest@miamioh.edu | 513-529-0360

Mount Vernon Nazarene University

• Bachelor of Science in Management Information Systems, Cybersecurity Concentration⁴⁹

Dr. Aaron Burgess | Assistant Professor of Management | Aaron.Burgess@mvnu.edu | 513.746-0726

North Central State College

• Associate of Applied Science in Information Technology – Cyber Security⁵⁰

³⁸ https://www.lorainccc.edu/it/associate-of-applied-science-in-computer-engineering-technology-computer-and-digital-forensicsmajor/

³⁹ <u>https://www.lorainccc.edu/it/associate-applied-science-cyber-information-security/</u>

⁴⁰ https://www.lorainccc.edu/it/computer-security/computer-information-systems-information-security-for-business-short-termcertificate/

- ⁴¹ <u>https://www.lorainccc.edu/it/computer-security/computer-information-systems-network-security-foundations-short-term-certificate/</u>
- ⁴² https://www.lorainccc.edu/it/computer-science-engineering-and-technology/computer-digital-forensics-one-year-certificate/

⁴³ <u>https://www.mtc.edu/course/cyber-security/</u>

⁴⁶ <u>https://www.mtc.edu/course/cyber-security/</u>

- ⁴⁸ <u>https://miamioh.edu/cybersecurity</u>
- ⁴⁹ <u>https://mvnu.edu/online/undergraduate/computer-sci/</u>

⁵⁰ https://ncstatecollege.edu/associate-degrees/information-technology-cyber-security/

⁴⁴ https://www.mtc.edu/course/networking/

⁴⁵ <u>https://www.mtc.edu/course/cit-networking-certificate/</u>

⁴⁷ https://www.malone.edu/academics/undergraduate/majors-minors/cybersecurity/

- Security Essentials Certificate⁵¹
- Network Security Essentials Certificate⁵²
- Network Security Administration/Management Certificate⁵³
- Cyber Security Network Defense Certificate⁵⁴

Carmen Morrison, M.I.S. | Assistant Professor/Program Coordinator, Information Technology | <u>cmorrison@ncstatecollege.edu</u>

Mohamed Ghonimy, M.S. | Assistant Professor, Cyber Security | <u>mghonimy@ncstatecollege.edu</u> | 419-755-4528

Northwest State Community College

- Associate of Cybersecurity and Network Administration⁵⁵
- Cybersecurity Short-Term Certificate⁵⁶

Ryan Hamilton | Dean, STEM and Industrial Technology Division | <u>rhamilton@NorthwestState.edu</u> | 419-267-1273

Tony Hills | Full-Time IT Faculty | thills@northweststate.edu | 419-267-1354

Notre Dame College

- Bachelor of Arts in Cybersecurity (also available online)⁵⁷
- Minor in Cybersecurity (also available online)⁵⁸

Florentine Hoelker | Dean, Finn Center for Adult, Online and Graduate programs | <u>fhoelker@ndc.edu</u> *Ken Palko* | Associate Professor and Chair, Arts and Humanities Division | <u>kpalko@ndc.edu</u> | 216-373-5296

Ohio Dominican University

• Bachelor of Science in Cybersecurity, Data Science, and Information Technology⁵⁹

Tom Brockman | Vice President for University Advancement and Marketing | <u>brockmat2@ohiodominican.edu</u> | 614-251-4453

The Ohio State University

• Bachelor of Science in Computer Science and Engineering – Focus in Information and Computation Assurance⁶⁰

Xiaodong Zhang | Critchfield Endowed Chair, Computer Science and Engineering | Zhang.574@osu.edu

Owens Community College

- Security Tech Certificate⁶¹
- Associate of Applied Science in Cybersecurity⁶²

Rhodes State College

• Cyber Security Certificate⁶³

⁵¹ https://www.ncstatecollege.edu/cms/certificates/security-essentials

⁵² <u>https://www.ncstatecollege.edu/cms/certificates/network-security-essentials</u>

⁵³ https://www.ncstatecollege.edu/cms/certificates/network-administration-management

⁵⁴ <u>https://ncstatecollege.edu/certificates/cyber-security-network-defense</u>

⁵⁵ <u>https://northweststate.edu/cybersecurity-network-administration</u>

⁵⁶ https://northweststate.edu/wp-content/uploads/files/20.02Cybersecurity-Certificate.pdf

⁵⁷ https://www.notredamecollege.edu/academicprograms/cybersecurity/

⁵⁸ <u>https://www.notredamecollege.edu/academicprograms/cybersecurity/</u>

⁵⁹ https://www.ohiodominican.edu/future-students/odu-news-events/news-item/2022/09/07/odu-introduces-newtechnology-focused-undergraduate-majors

⁶⁰https://cse.osu.edu/current-students/undergraduate/majors

⁶¹ https://www.owens.edu/academics/program/security-tech-cert.html

⁶² https://www.owens.edu/academics/program/cyber-security.html

⁶³<u>http://www.rhodesstate.edu/en/Current%20Students/Academic%20Programs/Division%20of%20Business%20Technology%20and%</u>20Public%20Service/Network%20Security/Cyber%20Security%20Certificate.aspx

• Associate of Applied Science in Network Security⁶⁴

Diane Miller | Chair, Information and Emerging Technology | Miller.D@RhodesState.edu | 419-995-8140

Shawnee State University

- Minor in Cybersecurity⁶⁵
- Associate in_Applied Business in Information Security⁶⁶
- Bachelor of Science in Information Security

Janice Johnson | Associate Professor and Chair, Department of Business | jjohnson@shawnee.edu | 740-351-3347

Sinclair Community College

- Associate of Applied Science--Cyber Investigation Technology⁶⁷:
- Associate of Applied Science-- Computer Information Systems/Secure System Administration⁶⁸
- Information Systems Security Short-Term Technical Certificate⁶⁹
- Network Engineering Security Associate Short-Term Technical Certificate⁷⁰
- Cyber Investigation One-Year Technical Certificate⁷¹

Kyle Jones | Associate Professor/Chair, Computer Information Systems Department | Kyle.jones4990@sinclair.edu | 937-512-2412

Southern State Community College

- Associate of Applied Science in Computer Technology with a focus in Cybersecurity⁷²
- Partnership with UC to earn a Bachelor of Science in Information Technology Cybersecurity⁷³

Josh Montgomery, M.I.S. | Associate Professor, Computer Science | jmontgomery@sscc.edu | 800-628-7722 ext. 3678

Stark State College

- Associate of Science in Cyber Security and Computer Forensics Technology⁷⁴
- Associate of Applied Science in Computer Network Administration and Security Technology⁷⁵

Dr. Larry Ray, PhD. | Department Chair, Information Technology| lray@starkstate.edu | 330-494-6170

Terra State Community College

 Associate of Applied Science in Systems and Networking Support (includes all of Terra State's cyber security courses)⁷⁶

⁶⁴http://www.rhodesstate.edu/Current%20Students/Academic%20Programs/Division%20of%20Business%20Technology%20and%20 Public%20Service/Network%20Security.aspx

⁶⁵ https://www.shawnee.edu/areas-study/college-professional-studies/business-administration/minors

⁶⁶ https://www.shawnee.edu/areas-study/college-professional-studies/business-administration/associate-degrees/information-security ⁶⁷ https://www.sinclair.edu/program/params/programCode/CYIT-S-AAS/

⁶⁸https://sinclair.edu/program/params/programCode/NEMA-S-AAS/

⁶⁹https://www.sinclair.edu/program/params/programCode/ISSC-S-STC/

⁷⁰https://www.sinclair.edu/program/params/programCode/NESA-S-STC/

⁷¹ https://sinclair.edu/program/params/programCode/CYSEC-S-CRT/

⁷² https://www.sscc.edu/academics/programs/computer-science.shtml

⁷³ <u>https://www.sscc.edu/academics/associate/computer-technology-uc-partnership.shtml</u>

⁷⁴ <u>https://www.starkstate.edu/academics/programs/cyber-security-and-computer-forensics-technology/</u>

⁷⁵ <u>https://www.starkstate.edu/academics/programs/computer-network-administration-and-security-technology/</u>

⁷⁶ <u>http://catalog.terra.edu/preview_program.php?catoid=3&poid=305&returnto=111</u>

Haley Crabtree, M.B.A. | Associate Professor, Computer Information Systems | <u>hcrabtree01@terra.edu</u> | 419-559-2314 *Abby Mever* | Academic and Career Advisor | <u>Amevers02@terra.edu</u>

Tiffin University

- Bachelor of Arts in Cyber Security⁷⁷
- Bachelor of Criminal Justice in Digital Forensics⁷⁸
- Master of Science in Cybersecurity⁷⁹
- Center for Cyber Defense & Forensics⁸⁰

David Selnick, M.A. | Vice Provost and Dean, School of Criminal Justice and Social Sciences | <u>selnickdj@tiffin.edu</u>

University of Akron

- Bachelor of Science in Computer Information Systems Cyber Security Option⁸¹
- Bachelor of Science in Computer Information Systems, Digital Forensics Technology Option⁸²
- Associate in Computer Information Systems (with security component)⁸³

Stanley Smith | Program Director, Computer Information Systems – Cybersecurity, Digital Forensics| <u>shsmith@uakron.edu</u> | 330-972-6950

University of Cincinnati:

- Certificate in Cyber Operations⁸⁴
- Certificate in Foundations of Cybersecurity⁸⁵
- Graduate Certificate in Cyber Operations⁸⁶
- Bachelor of Science in Information Technology Cybersecurity⁸⁷
- Bachelor of Science in Information Technology Cybersecurity Specialization (Online)⁸⁸
- Bachelor of Science in Cybersecurity Engineering⁸⁹
- Master of Science in Information Technology in Cybersecurity⁹⁰
- Online Master of Science in Information Technology in Cybersecurity⁹¹
- Master of Engineering, Artificial Intelligence & Cyber Security Concentration⁹²
- Master of Science in Computer Science, Cyber Operations Track⁹³

⁸⁷ https://cech.uc.edu/schools/it/academics/undergrad-

⁷⁷ https://www.tiffin.edu/cybersecurity

⁷⁸ <u>https://www.tiffin.edu/digital-forensics</u>

⁷⁹ https://www.tiffin.edu/academics/graduate/master-science/cyber-security

⁸⁰ <u>https://www.tucybercenter.org/</u>

⁸¹<u>https://www.uakron.edu/academics_majors/undergraduate/programs_detail.dot?programId=6f9338b4-154c-4a8c-bf43-</u>

⁸⁰⁰⁶ae0aa9df&pageTitle=Undergraduate majors&crumbTitle=Computer Information Systems | Cybersecurity (bachelor%27s degree) 82 https://bulletin.uakron.edu/undergraduate/colleges-programs/applied-science-technology/business-information-

technology/computer-information-systems-digital-forensics-technology-option-bs/#recommendedsequencetext

⁸³ <u>https://www.uakron.edu/academics_majors/undergraduate/programs_detail.dot?programId=e692db09-538e-4c64-bd39-</u>

³c3664afe2e6&pageTitle=Undergraduate majors&crumbTitle=Computer Information Systems (associate degree)

⁸⁴ https://webapps2.uc.edu/ecurriculum/degreeprograms/program/detail/20CRT-CYBR-C1

⁸⁵https://cech.uc.edu/schools/it/academics/undergrad-programs/foundations-of-cybersecurity.html

⁸⁶ https://webapps2.uc.edu/ecurriculum/degreeprograms/program/detail/20GC-CPCO-GC

programs/bachelorsofscienceininformationtechnology/bsinformatiotechnology.html

⁸⁸ https://cech.uc.edu/schools/it/academics/undergrad-programs/bachelorsofscienceininformationtechnology.html

⁸⁹ https://ceas.uc.edu/academics/departments/electrical-engineering-computer-science/degrees-programs/cybersecurityengineering-bachelor-of-science.html

⁹⁰ https://cech.uc.edu/schools/it/academics/grad-programs/masters-information-technology/Master-of-Science-in-Information-Technology.html

⁹¹ <u>https://online.uc.edu/programs/ms-information-technology/</u>

⁹² http://ceas.uc.edu/programs_degrees/MasterOfEngineering/degrees---on-campus.html#CS

⁹³ https://ceas.uc.edu/academics/departments/electrical-engineering-computer-science/degrees-programs/computer-science-master-of-science.html

- Master of Science in Cybersecurity Engineering⁹⁴
- Doctor of Philosophy in Computer Science and Engineering, Cyber Operations track⁹⁵

Teresa Hamad | Program Manager, College of Engineering and Applied Science | <u>hamadt@ucmail.edu</u> | 513-556-2833

Dr. Hazem Said, PhD. | Professor, School of Information Technology | <u>saidhm@ucmail.uc.edu</u> | 513-556-4874 *Dr. Marc M. Cahay, PhD.* | Professor and Department Head, Electrical Engineering & Computer Science | <u>cahaymm@ucmail.uc.edu</u> | 513-556-4754

University of Dayton

- Graduate Certificate in Cyber-Security Management⁹⁶
- Center for Cybersecurity & Data Intelligence⁹⁷
- Bachelor of Science in Business Administration, Management Information Systems with Minor in Cyber Security Management⁹⁸
- Bachelor of Arts in Criminal Justice, Cyber-Security Management Concentration⁹⁹
- Minor in Cyber Security Management¹⁰⁰
- Certificate in Cyber-Security Management¹⁰¹

Dr. John Mittelstaedt, PhD. | Dean and Professor, School of Business Administration | 937-229-3349 *Dr. Jayesh Prasad, PhD.* | Professor and Chairperson, Department of MIS, Operations Management, and Decision Sciences | <u>Prasad@udayton.edu</u>

Dr. Eric Balster, PhD. | Department Chair and Professor, Electrical and Computer Engineering | 937-229-3611 *Dr. Martha Henderson Hundley* | Professor and Director, Criminal Justice Studies Program | 937-229-2459 *Guru Subramanyam* | Professor, Joint Appointment with Bioengineering Graduate Program | <u>Gsubramanyam1@udayton.edu</u>

University of Findlay

- Bachelor of Science Degree in Computer Science with an emphasis in Information Assurance¹⁰²
- Certificate in Information Assurance¹⁰³
- Master of Science in Applied Security and Analytics¹⁰⁴

Dr. Helen Schneider, PhD. | Professor and Chair of Computer Science | schneider@findlay.edu | 419-434-4554

University of Mount Union

• Minor in Computer and Network Security¹⁰⁵

Blase Cindric | Department Chair and Associate Professor, Computer Science and Information Systems | <u>cindricbb@mountunion.edu</u> | 330-829-6649

⁹⁵ https://ceas.uc.edu/academics/departments/electrical-engineering-computer-science/degrees-programs/computer-scienceengineering-phd.html

⁹⁷ <u>https://www.udayton.edu/cybersecurity/</u>

- ⁹⁹ https://udayton.edu/artssciences/academics/criminaljustice/academics/criminal-justice-cyber.php
- ¹⁰⁰ https://udayton.edu/business/undergraduate-academics/cyber-security-management-minor.php
- ¹⁰¹ https://udayton.edu/business/graduate-academics/graduate_certificates/cyber_security.php
- ¹⁰² https://www.findlay.edu/sciences/computer-science/information-assurance
- ¹⁰³ <u>https://www.findlay.edu/sciences/applied-security-analytics-masters/information-assurance-certificate</u>
- ¹⁰⁴ <u>https://www.findlay.edu/sciences/ms-applied-security-analytics/</u>

 $^{^{94} \, \}underline{https://cech.uc.edu/schools/it/undergrad-programs/bachelor-cybersecurity/bachelor-cybersecurity-curriculum.html}$

⁹⁶ https://udayton.edu/business/graduate-academics/graduate_certificates/cyber_security.php

⁹⁸https://udayton.edu/business/undergraduate-academics/management-information-systems-bsba.php

¹⁰⁵<u>https://www.mountunion.edu/computer-and-network-science - :~:text=The computer and network security,skills through hands-on experience.&text=The minor in computer and,a program in computer science.</u>

University of Northwestern Ohio

• Associate of Applied Business in Network Security¹⁰⁶

Tim Fitzpatrick | Dean of the College of Business, Health, & Occupational Professions | tfitzpatrick@unoh.edu

University of Toledo

- Minor in Business Information Security (Cybersecurity)¹⁰⁷
- Master of Cyber Security¹⁰⁸
- Master of Science in Cybersecurity¹⁰⁹
- Graduate Certificate Program in Cyber Security¹¹⁰

Jeffrey Osthimer, M.Ed. | Chair and Associate Professor, Business Technology | <u>Jeffrey.osthimer@utoledo.edu</u> | 419-530-3357

Dr. Ahmad Y. Javaid, PhD. | Assistant Professor | <u>ahmad.javaid@utoledo.edu</u> | 419-530-8260 *Dr. Weiqing Sun, PhD.* | Program Director and Associate Professor, MS Cybersecurity Program | weigqing.sun@utoledo.edu | 419-530-3273

Valley College

- Cybersecurity Associate's Degree¹¹¹
- Cybersecurity Bachelor's Degree¹¹²

Warren County Career Center

• CompTIA Security+ Certificate¹¹³

Gary Patton | gary.patton@mywccc.org | 513-932-8145 ext. 5297

Washington State Community College

- Associate of Technical Studies in Cyber Security and Investigation¹¹⁴
- Cyber Security One-Year Technical Certificate

Dr. Adam Beatty, PhD. | abeatty@wscc.edu | 740-885-5725

Western Governors University:

- Bachelor of Science, Cybersecurity and Information Assurance¹¹⁵
- Master of Science, Cyber Security and Information Assurance¹¹⁶

Mike Morris, MAIS | Associate Director, Center for Cyber Education; Program Chair, Cybersecurity Programs | mike.morris@wgu.edu | 385-428-5554

Wittenberg University

• Bachelor of Computer Science with a Concentration in Cyber Security¹¹⁷

Dr. Adam Parker, PhD. | Professor of Mathematics, Chair of the Department of Mathematics and Computer Science | <u>aparker@wittenberg.edu</u> | 937-327-7864

¹⁰⁶ <u>http://www.unoh.edu/files/college-of-occupational-</u>

professions/Associate%20-%20Information%20Technology%20-%20Network%20Security.pdf

¹⁰⁷ <u>https://catalog.utoledo.edu/undergraduate/business-innovation/minors/business-information-security-cybersecurity/</u>

¹⁰⁸ <u>https://www.utoledo.edu/Programs/grad/Cyber-Security</u>

¹⁰⁹ https://www.utoledo.edu/Programs/grad/Cyber-Security

¹¹⁰ https://www.utoledo.edu/engineering/graduate-studies/cyber-certificate.html

¹¹¹ <u>https://valley.edu/programs/cybersecurity-training/</u>

¹¹² https://valley.edu/programs/cybersecurity-training/

¹¹³ https://www.mywccc.org/InformationTechnology1.aspx

¹¹⁴ http://www.wscc.edu/programs-and-certificates/ats/cyber-security.html

¹¹⁵ https://www.wgu.edu/online-it-degrees/cybersecurity-information-assurance-bachelors-program.html

¹¹⁶ <u>http://www.wgu.edu/online_it_degrees/cybersecurity_information_assurance_master_degree</u>

¹¹⁷ http://www.wittenberg.edu/academics/computerscience.html

Wright State University

- Certificate in Cyber Security Analytics¹¹⁸
- Associate of Applied Science in Information Technology and Cybersecurity
- Bachelor of Arts or Bachelor of Science in Computer Science with Cyber Security Analytics Certificate¹¹⁹
- Bachelor of Science in Information Technology and Cybersecurity¹²⁰
- Graduate level certificate in Cyber Security¹²¹
- Master of Science in Cyber Security¹²²

Dr. Brian D. Rigling, PhD. | Professor and Dean, College of Engineering and Computer Science | brian.rigling@wright.edu | 937-775-5001

Dr. Nathan W. Klingbeil | Professor, Mechanical and Materials Engineering | <u>nathan.klingbeil@wright.edu</u> | 937-775-5159

Youngstown State University

• Major in Computer Information Systems¹²³

Dr. Kriss Schueller | Professor and Acting Chair of Computer Science and Information Systems | kaschueller@ysu.edu

Zane State College

• Cybersecurity Associate Degree¹²⁴ Will Bailey | <u>wbailey@zanestate.edu</u>

¹¹⁸ https://engineering-computer-science.wright.edu/computer-science-and-engineering/cyber-security-analytics-undergraduatecertificate

¹¹⁹ <u>https://engineering-computer-science.wright.edu/computer-science-and-engineering/cyber-security-analytics-undergraduate-certificate</u>

¹²⁰<u>https://engineering-computer-science.wright.edu/computer-science-and-engineering/bachelor-of-science-in-information-technology-and-cybersecurity</u>

¹²¹ <u>https://engineering-computer-science-wright.edu/computer-science-and-engineering/cyber-security-analytics-graduate-certificate</u>

¹²² https://engineering-computer-science.wright.edu/computer-science-and-engineering/degrees-and-certificates/master-of-science-incyber-security

¹²³ <u>http://www.ysu.edu/academics/science-technology-engineering-mathematics/computer-information-systems-major</u>

¹²⁴ https://www.zanestate.edu/programs/it/cyber-aa/