Carleton University

Office of the Vice-Provost and Associate Vice-President (Academic)

memorandum

DATE: May 16, 2023

TO: Senate

FROM: Dr. Dwight Deugo, Vice-Provost and Associate Vice-President (Academic), and Chair, Senate Quality Assurance and Planning Committee

RE: 2023-24 Calendar Curriculum Proposals
Graduate Major Modification and Program Governance Change

Background

Following Faculty Board approval, as part of academic quality assurance, major curriculum modifications are considered by the Senate Quality Assurance and Planning Committee (SQAPC) before being recommended to Senate. Major curriculum modifications are also considered by the Senate Committee on Curriculum, Admissions and Studies Policy (SCCASP).

Library Reports (as required)

In electronic communication members of the Library staff, upon review of the proposals, confirmed no additional resources were required for the 2023-24 major modifications included below.

Documentation

Recommended calendar language, along with supplemental documentation as appropriate, are provided for consideration and approval.

Omnibus Motion

In order to expedite business with the multiple changes that are subject to Senate approval at this meeting, the following omnibus motion will be moved. Senators may wish to identify any of the major modifications that they feel warrant individual discussion that will then not be covered by the omnibus motion. Independent motions as set out below will nonetheless be written into the Senate minutes for those major modifications that Senators agree can be covered by the omnibus motion.

THAT Senate approve the major modifications as presented below.

Major Modifications

1. **MENG IPIS**
   SCCASP approval: May 2, 2023
   SQAPC approval: May 11, 2023

Senate Motion June 2, 2023

THAT Senate approve the introduction of the collaborative specialization in Cybersecurity to the MENG in Infrastructure Protection and International Security as presented with effect from Fall 2023.

2. **Undergraduate programs in Indigenous Studies**
   SCCASP approval: N/A
   SQAPC approval: May 11, 2023

Senate Motion June 2, 2023

THAT Senate approve the governance change to the Indigenous Studies programs as presented to take effect upon approval.

MEMORANDUM

To: Vice-Presidents' Academic and Research Council (VPARC)

From: Alex Wilner, Director, Infrastructure Protection & International Security (IPIS) program
Teddy Samy, Director, Norman Paterson School of International Affairs
Stephanie Carvin, Norman Paterson School of International Affairs (NPSIA)
Leah West, Norman Paterson School of International Affairs (NPSIA)
Jason Jaskolka, Systems and Computer Engineering (SCE)
Ashraf Matrawy, School of Information Technology (SIT)
Michel Barbeau, Director, School of Computer Science (SCS)

cc: Larry Kostiuk, Dean, Faculty of Engineering and Design
Maria DeRosa, Dean, Science
Brenda O'Neill, Dean, Faculty of Public Affairs
Patrice Smith, Dean, Faculty of Graduate and Postdoctoral Affairs
Dan Siddiqi, Associate Dean, Faculty of Graduate and Postdoctoral Affairs

Date: January 10, 2023

Subject: Major Modification Track A: New Collaborative Specialization in Cybersecurity

---

Modification Description

A new collaborative specialization in the area of cybersecurity at the master's level is being proposed. The collaborative specialization is intended to be interdisciplinary, bridging the study of international affairs and national security, computer science and engineering, and information technology.

The collaborative specialization will entail a new, cross-disciplinary, year-long (1.0 credit) course, compulsory for all students. CYBR 5000 *Science and Social Science of Cybersecurity* will offer students both a general overview of the legal, governance, and strategic considerations of cybersecurity from a Canadian and international perspective *and* a substantive understanding of the computer science and engineering concepts critical to effective cybersecurity operations. CYBR 5000 will be co-taught by one instructor from NPSIA and one from Systems and Computer Engineering (SCE), School of Information Technology (SIT), or School of Computer Science (SCS), or a Contract Instructor from Communications Security Establishment (CSE), which, importantly, already approaches the subject of cybersecurity from the necessary interdisciplinary perspective and has personnel currently teaching at NPSIA.

The specialization will allow for contributing programs to offer either a coursework or research pathway, or both. All pathways will require 1.0 credit in CYBR 5000. For the coursework pathway, students will be required to complete a 0.5 credit elective in an approved course with content relevant to the specialization. Students in the research thesis/essay pathway will complete the specialization by pursuing independent research in an area of cybersecurity.

Impact on Other Programs

To remain competitive with other Canadian universities and attract top-notch graduate students, and to better reflect larger changes taking place within society, Carleton must develop a cross-disciplinary program that bridges the disparate fields related to cybersecurity. The proposed specialization will add a foundational course in cybersecurity to all participating programs while leveraging ongoing and existing teaching and research excellence already taking place at Carleton. This will enrich existing programs in disciplines where cybersecurity is a growing and evolving consideration, while drawing more students to enroll in participating programs at Carleton.

The initial participating programs include:

Program	**Faculty**	**Unit**
M.A. International Affairs	FPA	Norman Paterson School of International Affairs
M.Infrastructure Protection & International Security	FPA/CIV	Infrastructure Protection and International Affairs
M.Eng Infrastructure Protection & International Security	FPA/CIV	Infrastructure Protection and International Affairs
M.A.Sc Electrical and Computer Engineering	FED	Department of Systems and Computer Engineering
M.Eng Electrical and Computer Engineering	FED	Department of Systems and Computer Engineering
M.I.T. Information Technology	FED	School of Information Technology
M.C.S	FS	School of Computer Science (SCS)

Impact on Learning Outcomes

Students who have completed the Collaborative Specialization in Cybersecurity will be able to:

1. Understand the cybersecurity challenge in a local, national, international context;
2. Discuss cybersecurity in all of its iterations, including from a geopolitical, national, legal, economic, and policy perspective and from a scientific, engineering, network, and informatics perspective;
3. Forecast the impact of emerging technologies on cybersecurity;
4. Apply a range of interdisciplinary methods for exploring and assessing cybersecurity challenges, opportunities, issues, and solutions;
5. Identify where the cybersecurity risk is most acute, and understand what tools (e.g., technology, legal, policy, financial) are available to address it, when, and in what order;
6. Describe the importance of cybersecurity for Canadian national and economic interests;
7. Identify innovative solutions to a wide range of cyber threats by drawing on the expertise of cybersecurity leaders in the private and the public sector;
8. Provide professional opportunities in a range of cybersecurity fields including in public policy, national security and defence, and engineering, computer science, and information technology.

In sum, Carleton's Cybersecurity Specialization will help develop well-rounded cybersecurity professionals with a range of comprehensive skillsets. It will help foster research into enduring or future technology and close existing gaps in skills, including in privacy protections, AI and automated cyber defence, open standards, quantum resistant security, and other related topics. Importantly, these issues are emerging in an era where there is growing concern about privacy, surveillance, and human rights within cyberspace; cyber is increasingly used by autocratic regimes as a tool for surveillance, disinformation and misinformation, and repression. Carleton's Cybersecurity Specialization will help students grapple with developing international norms, laws, and standards for cyberspace, and better consider the nexus between human rights, governance, and technology relating to a range of interdisciplinary topics, including, biases in artificial intelligence, cyber systems that are detrimental to marginalized and equity-deserving communities, the ethics of surveillance, and international law in cyber-space.

Societal Need

In the current national and geopolitical context, compounding factors underscore a growing concern for Canada's cybersecurity. The cybersecurity risk Canadians face is increasing year over year, as more individuals and organisations move on-line and more public and private services are digitised.[1] In tandem with this trend, the frequency and complexity of cyber threat are increasing. Statistics Canada has found, for illustration, that the percentage of Canadians reporting a cybersecurity incident rose from 52% in 2018 to 58% in 2020. Among the incidents most often reported were: receiving fraudulent emails or unsolicited spam (49%), getting redirected to fraudulent websites asking for personal information (20%), being targeted by a virus or other computer infection (10%) or being victimised by fraudulent payment card use (7%).[2] Moreover, an increasing number and range of malicious cyber actors now have relatively easy access to exploitation tools and tradecraft to access networks and on-line information for purposes of intelligence, profit, or intimidation.[3] It follows, then, that cyber compromises or incidents have and will continue to have an increased impact on Canadians and Canadian businesses as operations and services are disrupted, privacy is breached, IP or critical information is stolen, critical infrastructure is attacked, recovery costs soar and reputational damage is incurred. Ransomware is a particular pernicious threat. In

[1] Statistics Canada, Canadian Internet Use Survey, 2020; Statistics Canada, Digital Economy and Society Statistics.
[2] Canadian Internet Use Survey, 2020.
[3] Communications Security Establishment (2020), National Cyber Security Threat Assessment, 2020.

2021, 39% of businesses in Canada reported being hit by ransomware with each ransomware attack resulting in estimated average recovery cost of 2 million dollars.[4]

Exacerbating the situation is the global shortage of skills required to support cybersecurity cooperation across government and industry. Both the private sector and the public sector continue to struggle to find the cybersecurity professionals they need. A 2019 survey of IT decision makers across eight countries conducted by the Center for Strategic and Intelligence Studies found that 82% of employers report a shortage of cybersecurity skills, and 71% believe this talent gap causes direct and measurable damage to their organisations.[5] Canada has not been immune to this skills deficit.[6] A recent 2021 study conducted by (ISC)^2, an international non-profit cybersecurity professional association, estimates that Canada will need 25,000 new cybersecurity professionals in 2022-2023.[7]

The cybersecurity skills deficit manifests in two ways. There are a limited number of trained cybersecurity candidates available to hire. Two-thirds (60%) of participants in the (ISC)^2 study reported that a cybersecurity staffing shortage is placing their organisation at risk. Despite another influx of 700,000 professionals into the cybersecurity workforce, the study shows that global demand for cybersecurity professionals continues to outpace supply — resulting in a cybersecurity workforce gap. Participants reported that when cybersecurity staff is stretched thin, the negative consequences are real: misconfigured systems, slow patch cycles, rushed deployments, not enough time for proper risk assessment, not enough oversight of processes and procedures, and more.[8]

The skills deficit also manifests as a growing concern about the adequacy of the training prospective candidates receive prior to hiring. The (ISC)^2 report determined that the most effective professional training needs to *blend* technical skills, such as coding and vulnerability detection, with complementary "soft" skills in risk analysis, security governance, law and ethics, governance and policy, and compliance policy development.[9] Organisations have consistently noted that communication skills, the capacity to work in multi-disciplinary teams, and problem-solving skills are crucial attributes for cybersecurity professionals. Strong communication and writing skills enable these individuals to effectively translate technical insights into comprehensible, actionable direction to management.[10]

Canadian governments, industry and academia are all investing in cybersecurity. In the 2022 Federal Budget, over $850M was allocated to new cybersecurity initiatives on top of $750M provided in previous years.[11] On the surface, it appears that industry is trending toward improved awareness of and investments in cybersecurity. And yet today's emerging focus is still too narrow in scope: as cybersecurity challenges become more acute, technical skills and vulnerability research receive the lion's share of attention, at the expense of greater interdisciplinarity. While Canada has recently published an international law statement on the application of international law in cyberspace[12] and tabled legislation for critical cyber systems

[4] Aimee O'Driscoll, Comparitech Blog Canada Cyber Security and Cyber Crime Statistics (2020-2022) (August 1, 2022); Statistics Canada, The Daily, Types of cyber security incidents that impacted businesses, Canada.
[5] William Crumpler and James A. Lewis, The Cybersecurity Workforce Gap, Center for Strategic & International Studies, 2019.
[6] Rob Roshotte, Cybersecurity skills gap weakens cyber defences, IT World Canada, May 30, 2022.
[7] ISC, Cybersecurity Workforce Study 2021.
[8] Ibid.
[9] Ibid.
[10] Supra, Note 1.
[11] Government of Canada (2022), Budget 2022: Enhancing Canada's Cyber Security.
[12] Government of Canada (2022), Canada's Statement on International Law Applicable in Cyberspace.

protection,[13] there has been relatively limited public debate in Canada about the legal, ethical, policy and social aspects of cyber security.

Each of these requirements—investment, best practices, research, legal and policy development—are critical. But they are far more powerful when jointly planned and implemented by the full community of public and private sector cybersecurity stakeholders. Crucially, the more mature and integrated the approach, the better the impact, but also the greater the enhancement of Canada's position as a leader in cybersecurity on the international stage.

What is required is a new, horizontal, integrated, coherent approach where government, industry and academia partner together to create a whole-of-society approach that builds a national culture of cybersecurity. The proposed interdisciplinary cybersecurity specialisation will contribute to this process by offering students an environment that supports the development of the skills, research capability, and thought leadership needed to mature Canada's cybersecurity capabilities.

Student Demand

There is strong and growing student demand for education in cybersecurity internationally, in Canada, and at Carleton.

First, international university programs dedicated to cybersecurity continue to expand year over year. For illustration, in the United States the number of National Security Agency-designated Centers of Academic Excellence in Cybersecurity has expanded from seven in 2000 to nearly 400 in 2020.[14] Dozens of American universities have likewise recently established M.A. and Ph.D. programs in cybersecurity and related fields, often with support from major gifts and grants. For illustration, Johns Hopkins School of Advanced International Studies (SAIS), in partnership with the co-founder of CrowdStrike, an American cybersecurity and technology company, recently established The Alperovitch Institute for Cybersecurity Studies.[15] Its flagship program, the Master of Arts in Strategy, Cybersecurity, and Intelligence (MASCI), provides students with a one-year, interdisciplinary degree in cybersecurity.[16]

Second, a number of Canadian academic institutions have recently begun providing training related to cybersecurity. The government's Canadian Centre for Cyber Security lists dozens of examples, most in the form of technical diplomas, "microprograms", and graduate certificates.[17] Several graduate programs stand out, however:

- Concordia University offers both an M.A.Sc and M.Eng in Information Systems Security.[18]
- York University's Professional LLM program includes a distinct specialization in Privacy and Cybersecurity Law.[19]
- The University of Toronto's Identity, Privacy and Security Initiative (IPSI) offers an M.Eng in Communications with a focus on Identity, Privacy, and Security.[20]

[13] Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, 1st Session, 44th Parliament, 2022 (First reading June 14, 2022).
[14] Centers of Academic Excellence, National Centers of Academic Excellence In Cybersecurity, 2022 Edition.
[15] See: https://alperovitch.sais.jhu.edu/
[16] See: https://sais.jhu.edu/academics/master-degrees/master-arts-strategy-cybersecurity-and-intelligence-masci
[17] See: https://cyber.gc.ca/en/guidance/appendix-b-post-secondary-cyber-security-related-programs
[18] See: https://www.concordia.ca/ginacody/info-systems-eng/programs/information-systems-security/masc.html
[19] See: https://osgoodepd.ca/academic-programs/professional-llms/privacy-cybersecurity-law/
[20] See: http://www.ipsi.utoronto.ca/mengprogram.html

- The University of Ontario Institute of Technology's Faculty of Business and Information Technology offers a Master of Information Technology Security (MITS).[21]
- The University of Guelph, through the School of Computer Science, offers a Master of Cybersecurity and Threat Intelligence (MCTI).[22]
- Queen's University, in partnership with the Royal Military College, offers a cybersecurity graduate specialization.[23]
- The University of New Brunswick developed a Master of Applied Cybersecurity (MACSec), housed within the University's Canadian Institute of Cybersecurity (CIC).[24]
- The University of Victoria offers a Master of Engineering in Telecommunications & Information Security (MTIS)[25]

Importantly, unlike the proposed specialization at Carleton, most of these initiatives are not inter-disciplinary; they are rooted to a single school or department and address cybersecurity from one (rather narrow) perspective, law in the case of York's program, and computer science, engineering, and IT in the case of the others. The exceptions include Queen's specialization and the MITS program at Ontario Tech University, though both only require that students take one social science class. **That no Canadian university has yet developed an interdisciplinary cybersecurity specialization or graduate program suggests that Carleton has an opportunity to leverage our existing expertise and national reputation in the fields of computer science, information technology, international affairs and infrastructure protection and international security.**

Third and finally, demand for cybersecurity courses at Carleton is growing steadily. NPSIA's and IPIS's core classes on the subject – INAF 5225 [0.5] *Cybersecurity in Canada* and IPIS 5509 [0.5] *Introduction to Cybersecurity* – reach capacity within hours of registration and regularly turn away waitlisted students. In *Capstone in Canadian Security Policy*, INAF 5254 [0.5], students regularly over-subscribe for projects dedicated to emerging technology and cybersecurity, at the expense of other, more traditional projects. Other units have had similar experiences. In Systems and Computer Engineering, for instance, SYSC 5805 [0.5] *Security Engineering* has been regularly over-subscribed with as many as 50 students in each year it has existed. Consider, finally, that the Government of Canada, including the Communications Security Establishment and Public Safety Canada, more specifically, hires several Carleton graduate students every year on cybersecurity policy and law, often by directly approaching professors for insight on how to attract Carleton's best and brightest graduates.

Resources

The Collaborative Specialization in Cybersecurity will be managed by NPSIA. NPSIA is a diverse unit, with scholars of international law, political science, and economics. It boasts Carleton's largest graduate program. And, importantly, it has deep connections with the Government of Canada and the federal public service, which it uses to attract students, identify contract instructors, recruit research fellows, and help support research and scholarship. IPIS, which NPSIA administers, is equally diverse, managing two masters degrees (M.Eng IPIS and M.IPIS) with staff, faculty, and CIs from the School of International Affairs and the Faculty of Engineering and Design (FED). A NPSIA faculty member serves as IPIS Director.

[21] See: https://ontariotechu.ca/programs/graduate/business-and-information-technology/master-of-information-technology-security/index.php

[22] See: https://www.uoguelph.ca/computing/graduates-graduate-programs/master-cybersecurity-and-threat-intelligence-mcti

[23] See: Program Overview – NSERC CREATE Cybersecurity Program (queensu.ca)

[24] See: https://www.unb.ca/fredericton/cs/grad/masters/macsec/index.html

[25] See: https://www.uvic.ca/ecs/ece/future/mtis/index.php?utm_medium=redirect&utm_source=/engineering/ece/future/mtis/index.php&utm_campaign=redirect-usage

Both NPSIA and IPIS offer several courses on cybersecurity, and on the emerging nexus between technology, governance, law, economics, and policy. The day-to-day operations of the Collaborative Specialization will be managed by NPSIA's IPIS Director.

A *Cybersecurity Governance Committee* will oversee academic matters related to the specialization (e.g., calendar changes, identifying and recruiting CIs, program expansion, etc.). The governance committee will include the Director and/or a faculty representative from each participating academic program, including IPIS, NPSIA, SCE, SIT, and SCS. The Specialization will also include a *Board of Cybersecurity Advisors*, made up of 7 to 10 public and private sector cybersecurity professionals. Several such professionals have already indicated informally an interest in serving on such a Board, including Shelly Bruce (ret.) Chief, Communications Security Establishment, and Vincent Rigby (ret.), National Security and Intelligence Advisor, Prime Minster of Canada. Advisors will meet annually and as needed to help the Governance Committee better understand the evolving nature of cybersecurity, help fine-tune the specialization's teaching and research focus, help identify and recruit students, fellows, and CIs, and generate collaborative research opportunities.

The required resources for the Collaborative Specialization include one 1.0-credit Contract Instructor to replace faculty instructors and/or to co-teach the core course. This proposal assumes that no new resources are required for administrative staff or course releases for the Director. IPIS administrative staff will be sufficient for the launch of the program.

Program Change Request

New Program Proposal

Date Submitted: 04/18/23 10:45 am

Viewing: **TBD-2199 : M.Eng. Infrastructure Protection and International Security with Collaborative Specialization in Cybersecurity**

Last edit: 04/18/23 10:45 am

Last modified by: sandrabauer

Changes proposed by: sandrabauer

In Workflow

1. **IPIS ChairDir GR**
2. **ENG Dean**
3. **GRAD Dean**
4. **PRE GRAD FCC**
5. **GRAD FCC**
6. **GRAD FBoard**
7. **PRE SCCASP**
8. SCCASP
9. SQAPC
10. Senate
11. CalEditor

Approval Path

1. 04/18/23 11:47 am
Alex Wilner (alexwilner): Approved for IPIS ChairDir GR
2. 04/18/23 4:01 pm
Richard Dansereau (richarddansereau): Approved for ENG Dean
3. 04/18/23 4:02 pm
Sandra Bauer (sandrabauer): Approved for GRAD Dean
4. 04/19/23 11:17 am
Sandra Bauer (sandrabauer): Approved for PRE GRAD FCC
5. 04/19/23 11:18 am
Sandra Bauer (sandrabauer): Approved for GRAD FCC
6. 04/19/23 11:22 am
Sandra Bauer (sandrabauer): Approved for GRAD FBoard

Effective Date	2023-24
Workflow	majormod
Program Code	TBD-2199

Level	Graduate
Faculty	Faculty of Engineering and Design
Academic Unit	Infrastructure Protection and International Security
Degree	Master of Engineering
Title	M.Eng. Infrastructure Protection and International Security with Collaborative Specialization in Cybersecurity

Program Requirements

M.Eng. Infrastructure Protection and International Security with Collaborative Specialization in Cybersecurity (5.0 credits)

Requirements - Research project pathway:

1. 1.0 credit in:		1.0
CYBR 5000 [1.0]	Science and Social Science of Cybersecurity	
2. 1.5 credits in:		1.5
IPIS 5101 [0.5]	Critical Infrastructure Protection: Issues and Strategies	
IPIS 5105 [0.5]	Critical Infrastructure Risk Assessment	
IPIS 5106 [0.5]	Management of Critical Infrastructure	
3. 0.5 credit from:		0.5
IPIS 5104 [0.5]	Terrorism and International Security	
IPIS 5301 [0.5]	Disarmament, Arms Control and Nonproliferation	
IPIS 5302 [0.5]	Contemporary International Security	
IPIS 5303 [0.5]	Intelligence Statecraft and International Affairs	
IPIS 5304 [0.5]	Intelligence and National Security: Policies and Operations	
IPIS 5305 [0.5]	National Security Policy and Law	
IPIS 5306 [0.5]	Emergency and Business Continuity Management	
IPIS 5320 [0.5]	Topics in Infrastructure Security Policy	

Or 5000-level courses from the Intelligence and International Affairs (IIA) and Security Defence Policy (SDP) designated fields offered by the Norman Paterson School of International Affairs.

4. 1.0 credit from:		1.0
IPIS 5501 [0.5]	Transportation and Aviation Security	
IPIS 5504 [0.5]	Fundamentals of Fire Safety	
IPIS 5505 [0.5]	Natural Hazards in Canada: Risk and Impact	
IPIS 5507 [0.5]	Blast-load Effects on Structures	
IPIS 5508 [0.5]	Introduction to Explosives and Explosion Effects as they relate to Infrastructure and its Components	
IPIS 5509 [0.5]	Introduction to Cybersecurity	
IPIS 5520 [0.5]	Selected Topics in Engineering of Critical Infrastructure	

or an engineering course approved by the IPIS Director or Associate Director.

5. 1.0 credit in:	1.0

IPIS 5907 [1.0]	Research Project (in the area of the specialization)	
Total Credits		5.0

Requirements - Coursework pathway:

1. 1.0 credit in:		1.0
CYBR 5000 [1.0]	Science and Social Science of Cybersecurity	
2. 1.5 credits in:		1.5
IPIS 5101 [0.5]	Critical Infrastructure Protection: Issues and Strategies	
IPIS 5105 [0.5]	Critical Infrastructure Risk Assessment	
IPIS 5106 [0.5]	Management of Critical Infrastructure	
3. 1.0 credit from:		1.0
IPIS 5104 [0.5]	Terrorism and International Security	
IPIS 5301 [0.5]	Disarmament, Arms Control and Nonproliferation	
IPIS 5302 [0.5]	Contemporary International Security	
IPIS 5303 [0.5]	Intelligence Statecraft and International Affairs	
IPIS 5304 [0.5]	Intelligence and National Security: Policies and Operations	
IPIS 5305 [0.5]	National Security Policy and Law	
IPIS 5306 [0.5]	Emergency and Business Continuity Management	
IPIS 5320 [0.5]	Topics in Infrastructure Security Policy	

Or 5000-level courses from the Intelligence and International Affairs (IIA) and Security Defence Policy (SDP) designated fields offered by the Norman Paterson School of International Affairs.

4. 1.0 credit from:		1.0
IPIS 5501 [0.5]	Transportation and Aviation Security	
IPIS 5504 [0.5]	Fundamentals of Fire Safety	
IPIS 5505 [0.5]	Natural Hazards in Canada: Risk and Impact	
IPIS 5507 [0.5]	Blast-load Effects on Structures	
IPIS 5508 [0.5]	Introduction to Explosives and Explosion Effects as they relate to Infrastructure and its Components	
IPIS 5509 [0.5]	Introduction to Cybersecurity	
IPIS 5520 [0.5]	Selected Topics in Engineering of Critical Infrastructure	

or an engineering course approved by the IPIS Director or Associate Director.

5. 0.5 credit in approved electives in the area of the specialization

6. 0.5 credit from graduate courses from the Faculty of Engineering and Design that have been selected in consultation with, and approved by, the MIPIS Director and Associate Director. 0.5

Total Credits 5.0

New Resources	No New Resources
Summary	Late addition - Add M.Eng. IPIS with Collaborative Specialization in Cybersecurity
Rationale	See executive summary - this item was inadvertently omitted from the original package of Cybersecurity specializations to go forward for 23-24
Transition/Implementation	New program
Program reviewer comments	**sandrabauer (04/19/23 11:18 am):** Approved by email vote April 19, 2023 **sandrabauer (04/19/23 11:45 am):** FGPA Programs and Planning committee approved by email vote April 19, 2023. Subsequently approved at April 19, 2023 GFB meeting.

Key: 2199

Template for Major Modification A1: Change in Governance

MEMORANDUM

To: Vice-Presidents' Academic and Research Committee (VPARC) for A1s

From: Susan Ross, School of Indigenous and Canadian Studies; Julie Garlen, Institute of Interdisciplinary Studies

CC: Pauline Rankin, Dean of FASS; Peter Thompson, Associate Dean (Academic), FASS

Date: April 6, 2023

Subject: Major Modification to Indigenous Studies Programs. Track A1

Modification Description

Indigenous Studies has grown dramatically at Carleton since 2016. At that time, the School of Canadian Studies developed a Combined Honours degree in Indigenous Studies and subsequently changed its name to the School of Indigenous and Canadian Studies (SICS). During this period, the School's complement of Indigenous Studies scholars grew from one faculty member (on a limited term appointment) to six members who have at least 25% of their teaching appointed to the unit. As Indigenous Studies has expanded, it has become clear over time that the research and teaching priorities of the program have shifted away from an overriding focus on the relationship between Indigenous peoples and the Canadian settler state to a broader and more global understanding of Indigenous Studies.

In order to facilitate this shift in scholarly focus and to set in motion a longer-term plan of developing an autonomous Indigenous Studies unit, faculty members in the Indigenous Studies program have requested that governance of the program relocate from SICS to the Institute of Interdisciplinary Studies (IIS). In a March 10, 2023 letter to Pauline Rankin, Dean of FASS, Indigenous Studies faculty members wrote: "we as a collective have articulated a vision for the Indigenous Studies program that centers Critical Indigenous Studies, Global Indigenous Studies, IBPOC solidarities, Two-Spirit and Indigiqueer Stuides, and land-based learning, among others. At this time, we strongly feel that this vision is not achievable within the current structure of SICS. We are gearing up to launch our stand-alone BA this upcoming fall and would like the opportunity to continue to develop and grow the program with more agency." This memo proposes that the Indigenous Studies program move from SICS to IIS, which will allow the program to broaden its focus and to develop administrative structures that will further the program's ultimate goal of building a stand-alone unit.

The Dean of FASS, Pauline Rankin; the Associate Vice President, Indigenous Teaching, Learning, and Research, Kahente Horn-Miller; the Director of SICS, Susan Ross; and the Director of the Institute of Interdisciplinary Studies, Julie Garlen, each support this proposal.

This proposal does not affect the curriculum of the Indigenous Studies program. The major change is that the administrative home of Indigenous Studies will shift to the Institute of Interdisciplinary Studies. This change will have no impact on learning outcomes. The Indigenous Studies program will fit well within the current administrative structure of IIS, which features a Director and Associate Director who oversee and administer the two existing interdisciplinary B.A. programs. This structure will provide additional administrative support for the B.A. in Indigenous Studies as it grows.

Impact on Other Programs

This change will have minimal impact on other programs at the university. Courses within Indigenous Studies that are cross-listed with Canadian Studies and other programs will stay in place. Faculty in Indigenous Studies will retain their graduate supervisory privileges in other units, including Canadian Studies.

Resources

a. *Dean and Faculty Affiliation*: The program will remain in the Faculty of Arts. Responsibility for tasks such as timetabling, requests for new positions, CourseLeaf entries, and quality assurance will shift to the Institute of Interdisciplinary Studies.

b. *Faculty resources*: Will there be any changes to faculty affiliations or workload as a result of this governance change? Faculty affiliations will also shift to the Institute of Interdisciplinary Studies, but there will be no changes to workload as a result of this change in governance. The distribution of courses may shift over time, as Indigenous Studies faculty may find opportunities to teach in programs in IIS (Childhood and Youth Studies and Human Rights and Social Justice), but the expectations around workload remain the same.

c. *Administrative support*: The Dean of FASS is committed to ensuring that both units retain appropriate administrative support for their programs.

d. *Space*: SICS and IIS are contiguous: SICS is on the 12th floor of Dunton Tower and IIS is on the 13th floor. As a result, no offices will move as part of this governance change. Student space is available on the 13th floor for IIS programs. Indigenous Studies does not currently have graduate programs so there is no need for additional graduate student space at this time.

Appendix A:

Please include the modified Section C: Governance from your most recent Cyclical Program Review Self-Study or from your New Program proposal.

APPENDIX A

A. Governance

The program will be housed in the Institute of Interdisciplinary Studies (IIS). IIS has a Director and Associate Director who oversee and administer the Institute's interdisciplinary B.A. programs. The Director of IIS will be responsible for budget, scheduling, setting committee assignments, and speaking on behalf of the program at meetings such as Chairs and Directors and at Tenure and Promotion meetings. The Director and the Associate Director collaborate with faculty members in each area on the day-to-day operations of the Institute's programs, including curriculum and program changes, assisting students with course choices, and recruiting, community engagement, and promotional efforts. The Institute holds regular meetings of faculty appointed across the various programs and program-level meetings take place as needed. Like the rest of the programs in IIS, Indigenous Studies faculty will form a "committee of the whole" within the overarching structure of the Institute and will give direction to the Director and Associate Director on decisions relating to curriculum, governance, and hiring (including Contract Instructor hiring). Faculty members in Indigenous Studies will determine appropriate mechanisms for communication with the Indigenous Education Council, the Centre for Indigenous Support and Community Engagement and other organizations within Carleton and in the wider community.

~~The program will be housed in the School of Canadian Studies.~~

~~The Combined Honours and Minor will have a Program Coordinator, its own Program Committee and its distinct Committee of Management. The Director of the SCS will be responsible for budget, scheduling, setting committee assignments in consultation with the Program Coordinator, and will speak on behalf of the program at meetings such as Chairs and Directors and at tenure hearings. However, the day to day operations of the program will be administered by the Coordinator of the Indigenous Studies program and the undergraduate administrator from the School of Canadian Studies. The role of the Coordinator will be to institute and oversee curriculum and program changes, to assist students with their course choices, to liaise with the Director of the School of Canadian Studies and the Aboriginal Education Council, to lead recruiting, community engagement and promotional efforts, to represent the program within the departmental assembly, the university and the larger community.~~

~~While the coordinator will have executive power, legislative power will reside in the Indigenous Studies Programming Committee and, to a lesser extent, the Committee of Management. The Indigenous Studies programming committee will typically consist of the Coordinator and two or three faculty members directly involved in the delivery of INDG courses. The role of the programming committee will be to suggest curricular and programming changes and to help to develop recruiting, community engagement and promotional strategies.~~

~~In fulfilling those roles, the Indigenous Studies Programming Committee will consult regularly with the Committee of Management. This will be an advisory body composed of faculty and staff members from~~

~~across the university who work in the area of Indigenous Studies as well as students, traditional knowledge-holders, members of Indigenous organizations and activists, artists and practitioners. We will aspire to include First Nations, Métis and Inuit peoples in the Committee and we anticipate that there will be a strong overlap between the Committee of Management and the membership of the Aboriginal Educational Council as well as that of CIRCLE (The Centre for Indigenous Research, Culture, Language and Education).~~