

**UNIVERSITY OF WATERLOO
SENATE GRADUATE & RESEARCH COUNCIL
NOTICE OF MEETING**

DATE: Monday 14 November 2022
TIME: 10:30 a.m. – 12:00 noon
PLACE: NH 3318/3308

Chair – C. Dean

AGENDA

<u>Item</u>	<u>Action</u>
Declarations of Conflict of Interest a. Excerpt from Bylaw 1, section 8*	Information
<u>CONSENT AGENDA</u>	
Motion: To approve or receive for information by consent, items 1-2 below	
1. Minutes of 3 October 2022*	Decision (SGRC)
2. Graduate Awards*	
a. Faculty of Arts Research and Travel Grants Fund - trust	Decision (SGRC)
b. Students-At-Risk Bursary - trust	Decision (SGRC)
c. Soprema Canada Inc. Award – Tomorrow’s Leaders - trust	Information
d. Robert Ewen Philosophy Awards Fund - endowment	Information
<u>REGULAR AGENDA</u>	
3. Business Arising from the Minutes	Information
4. Co-chairs’ Remarks	Information
5. Digital Learning Principles and Guidelines* (David DeVidi, Aldo Caputo, Dina Meunier)	SEN-Regular
6. Research Centres and Institutes: Renewal-Cybersecurity and Privacy Institute* (N. Asokan)	Decision (SGRC)
7. Academic Program Reviews	
a. Final Assessment Report: Master of Catholic Thought* (Carol Ann MacGregor)	Decision (SGRC)
b. Final Assessment Report: Doctor of Optometry and Vision Science* / Two-year Progress Report: Doctor of Optometry and Vision Science* (Stan Woo)	Decision (SGRC) Decision (SGRC)
c. Two-year Progress Report: Graduate Diploma in Climate Risk Management* (Johanna Wandel)	Decision (SGRC)
8. Quality Council Update (Amanda McKenzie)	Information
9. Curricular Submissions	
a. Health* (Brian Laird)	Decision (SGRC)
10. Other Business	Information
11. Next Meeting: 12 December 2022 from 10:30 a.m. - 12 noon; NH3318	Information

*material attached
** to be distributed separately
“SGRC” to be approved on behalf of Senate
“SEN” to be recommended to Senate for approval

7 November 2022

Kathy Winter, PhD, CPsych
Assistant University Secretary

Excerpt from Senate Bylaw 1

8. Declarations of conflict of interest

8.01	At the beginning of each meeting of Senate or any of Senate’s committees or councils, the chair will call for members to declare any conflicts of interest with regard to any agenda item. For agenda items to be discussed in closed session, the chair will call for declarations of conflict of interest at the beginning of the closed portion of the meeting. Members may nonetheless declare conflicts at any time during a meeting.
8.02	A member shall be considered to have an actual, perceived or potential conflict of interest, when the opportunity exists for the member to use confidential information gained as a member of Senate, or any of Senate’s committees or councils, for the personal profit or advantage of any person, or use the authority, knowledge or influence of the Senate, or a committee or council thereof, to further her/his personal, familial or corporate interests or the interests of an employee of the university with whom the member has a marital, familial or sexual relationship.
8.03	Members who declare conflicts of interest shall not enter into debate nor vote upon the specified item upon which they have declared a conflict of interest. The chair will determine whether it is appropriate for said member to remove themselves from the meeting for the duration of debate on the specified item(s).
8.04	Where Senate or a committee or council of Senate is of the opinion that a conflict of interest exists that has not been declared, the body may declare by a resolution carried by two-thirds of its members present at the meeting that a conflict of interest exists and a member thus found to be in conflict shall not enter into debate on the specified item upon which they have declared a conflict of interest. The chair will determine whether it is appropriate for said member to remove themselves from the meeting for the duration of debate on the specified item(s).

University of Waterloo
SENATE GRADUATE & RESEARCH COUNCIL
Minutes of the 3 October 2022 Meeting
[in agenda order]
Needles Hall 3318/3308

Present: Steven Bednarski (for Drysdale), Jeff Casello, Amelia Clarke, Peter Deadman, Charmaine Dean, Bernie Duncker, Anna Esselment, Bertrand Guenin, Alison Hitchens, Julie Joza, Ian Milligan, Liz Nilsen, Jennifer Reid, Marianne Simm, Siva Sivoththaman, Mike Szarka, Kathy Winter (secretary).

Resources: Angela Christelis, Trevor Clews, Carrie MacKinnon, Amanda McKenzie.

Guests: Jennifer Coghlin, Shavin Malhotra, Richard Wikkerink.

Regrets: David Clausi*, Ana Ferrer*, Aiden Huffman, Brian Laird, Anita Layton, William McIlroy, Martin Ross, Julian Surdi, John Thompson, Shawn Wettig.

Organization of Meeting: Jeff Casello, co-chair of the council, took the chair, and Kathy Winter acted as secretary. The secretary advised that due notice of the meeting had been given, a quorum was present, and the meeting was properly constituted.

DECLARATIONS OF CONFLICT OF INTEREST

No conflicts of interest were declared.

CONSENT AGENDA

Council heard a motion to approve or receive for information the items of the consent agenda. Hitchens and Milligan. Carried.

1. MINUTES OF 12 September 2022

Council approved the minutes of the meeting as distributed.

2. RESEARCH ETHICS

Council approved a membership update and revision to the Clinical Research Ethics Board Terms of Reference as presented.

REGULAR AGENDA

3. BUSINESS ARISING FROM THE MINUTES

There was no business arising.

4. CO-CHAIRS' REMARKS

Dean updated council regarding: (a) deferred maintenance and renovations (being discussed at Office of Research in terms of maintenance funds required in order to meet needs outlined in grant applications, such as CFI) and (b) upcoming competitions (Canada First Research Excellence Fund, Canada Excellence Research Chairs competition, and Canada Biomedical Research Fund competition in which Ontario submitted a proposal).

Casello updated council regarding: (a) postdoctoral programs ([black and indigenous scholars](#), [AMTD](#), and [interdisciplinary postdoctoral program](#)), (b) Policy 30 – Employment of gradient student teaching assistants (in final reading and approval stages), (c) forthcoming campus Ombuds Office to serve campus community, and (d) international events and integrated campus response (central administration, faculty, student associations).

5. OFFICE OF THE REGISTRAR - ACADEMIC CALENDAR DATES 2023-24

Council heard a motion to recommend to Senate approval of the academic calendar dates for 2023-2024 and guidelines for determining academic calendar of dates, as presented. Deadman and Reid. Carried.

6. NEW PROGRAM: DOCTOR OF PHILOSOPHY IN ENTREPRENEURSHIP AND ORGANIZATION.

Council heard a motion to recommend to Senate to approve a new research-based Doctor of Philosophy in Entrepreneurship and Organization, offered by the Conrad School of Entrepreneurship and Business in the Faculty of Engineering, as presented. The PhD program will include course work, a comprehensive examination, a thesis proposal, and a thesis. The program will charge tuition consistent with all other PhD programs at the institution and will be delivered as a full-time program on-campus. Shavin Malhotra, Professor of Strategy & Conrad Research Excellence Chair, provided an overview of the new program and council discussed: synergy between job advertisements and program description, transfer payment entrepreneurship fellowships and scholarships, format is research-based with community collaboration in terms of data collection and invited speaker fora. Sivoththaman and Esselment. Carried.

7. CONSULTATION PLAN – SENATE GOVERNANCE REVIEW: FUTURE OF SGRC

Casello reminded council of the [Senate Governance Review](#)—in which all committees of Senate will participate. Members are to anticipate invitations to separate stakeholder consultation sessions to be held beginning this fall with a view to examine recommendations #28, #32, #33.

8. CURRICULAR SUBMISSIONS

Faculty of Mathematics.

On behalf of Senate, council approved new courses, new milestones, and minor program revisions for Combinatorics and Optimization (Guenin and Esselment. Carried), and Data Science (Guenin and Sivoththaman. Carried), as presented.

Council heard a motion to recommend to Senate major program revisions for Pure Math (Guenin and Sivoththaman. Carried), Combinatorics and Optimization (Guenin and Esselment. Carried), and Data Science (Guenin and Sivoththaman. Carried), as presented.

9. OTHER BUSINESS

There was no other business.

10. FUTURE BUSINESS

Council was reminded of topics for future strategic discussion: Create Grants, Jean Becker's What it Means to Decolonize and Institution, and GSPA Vision Document—the latter of which is anticipated to come forward at December 2022 SGRC. Visioning thereon to include topics such as differentiating elements of graduate studies, research, bibliometrics, vibrant student experience (both while studying and when transitioning to alumni, as well as fostering connections between alumni and current students). Council was invited to submit ideas for other topics for discussion to either co-chairs or SGRC secretary.

11. NEXT MEETING

The next meeting will be held Monday 14 November 2022 from 10:30 a.m. to 12 noon in NH3318.

18 October 2022

Kathy Winter, PhD, CPsych,
Assistant University Secretary



October 31, 2022

TO: Kathy Winter, Assistant University Secretary and Privacy Officer, Senate Graduate and Research Council

FROM: Heidi Mussar, Associate Director, Graduate Financial Aid & Awards

RE: Agenda items for Senate Graduate & Research Council – November 2022

Items for Approval

a) Faculty of Arts Research and Travel Grants Fund - trust

Awards are available to graduate students registered full time in a research-based master's or PhD program in the Faculty of Arts. Students should have a cumulative average of 80% or higher in their program. Activities that are eligible for awards include travel and accommodation for: conference participation where students will be presenting their own research; field work or archival research; or a work placement or internship. Interested students must complete an online application form found on the Faculty of Arts website. Selection will be made by the Arts Graduate Office. Applications will be accepted anytime throughout the year but must be received at least one month in advance of the travel or research activity.

The value of each award will vary depending on the specific budget requirements for the experience and the availability of funds. Students will normally be awarded an amount to help cover their costs rather than covering the full cost of the activity.

b) Students-At-Risk Bursary – trust

Through generous donations, limited funding is available to support students registered at the University of Waterloo who have had their program of study disrupted by conflict, war or changing political environments in their country of origin or where they were last registered prior to relocating to Waterloo to continue their program. Eligible applicants must submit an application by January 16, 2023.

Approx \$127k is available to be split between eligible graduate and undergraduate students.

Items for Information

c) Soprema Canada Inc. Award – Tomorrow's Leaders – trust

Originally approved at SG&RC in April 2019, the award is being renewed with a few minor revisions:

- Award name has been updated from "Soprema Award: Tomorrow's Leaders" to "Soprema Canada Inc. Award – Tomorrow's Leaders".
- A couple of the courses that eligible students needed to be enrolled in have been updated: ARCH 673 and 693 have been replaced by ARCH 671 and 691.
- Selection will normally be made in spring term instead of winter term.

The rest of the criteria remains the same as originally approved.

Renewed period of gift is 2023 to 2027.

d) Robert Ewen Philosophy Awards Fund – endowment

Originally approved at SG&RC in September 2019, the fund is being amended to expand the use of the fund.

Original purpose:

The goal is to provide funding to support the annual Philosophy Department Awards Program. Funds will support awards and prizes that recognize and reward academic achievement and/or commitment to the Department or its communities. The awards program is open to full-time undergraduate and graduate students registered in the Philosophy department and includes awards such as, but not limited to, class prizes, citizenship prizes, essay prizes, needs-based awards and travel awards. The Department of Philosophy will normally identify candidates and select recipients.

Revised purpose now includes the above plus:

Where available earnings exceed funding requirements to support the Philosophy Awards program in any given year, funds may be directed to support the continuation and further development of other Philosophy Department programs, initiatives and or activities.

For Recommendation**Public****Open Session**

To: **Senate Graduate and Research Council**

Sponsor: David DeVidi, Associate Vice-President, Academic
Contact Information: david.devidi@uwaterloo.ca

Presenter: Aldo Caputo, Director, Centre for Extended Learning
Contact Info: acaputo@uwaterloo.ca

Date of Meeting: **November 14, 2022**

Item Identification:

Digital Learning Principles and Guidelines

Summary:

The Associate Vice-President, Academic (AVPA) is bringing a Digital Learning Principles and Guidelines framework forward to address some needs that have become evident since the start of the Covid-19 pandemic. The framework is in two parts:

1. A set of *Principles and Guidelines* are articulated that are intended to serve as both baseline and guidelines for digital teaching and learning at Waterloo with the goal of ensuring that digital teaching and learning is done in a manner that complies with university policies and Canadian law, meets Waterloo's standards for quality, and clearly communicates to students the expectations around mode of delivery.
2. The framework also outlines a *Review and Approval Process*, but these are procedural matters that do not require Senate approval in the same way. Accordingly, this part of the Framework is for information.

Recommendation/Motion:

That council recommend to Senate the approval of the Principles and Guidelines for Digital Learning, as presented.

Jurisdictional Information:

This item is being submitted to Senate Graduate and Research Council in accordance with [Senate Bylaw 2](#); section 4.03(c).

Governance Path:

1. UOPS (12 April 2021): Aldo Caputo (Director, Centre for Extended Learning; CEL), presents the concept of developing a framework and the rationale to UOPS and receives support to proceed.
2. CEL works internally to develop first draft of framework; Keep Learning Team is consulted and helps revise the draft.
3. AVPA provides feedback.
4. UOPS (23 June 2022): framework presented; UOPS recommends progression to SUC.
5. SUC (4 October 2022): framework presented for discussion; SUC provides feedback and supports motion to recommend to Senate the approval of the framework *Principles and Definitions*.
6. Framework refined based on SUC feedback.
7. DC+ (19 October 2022): framework presented at Deans' Council Plus.

Previous Action Taken:

Described above in section entitled "Governance Path".

Highlights/Rationale:

The need for such a framework has become clear because of the greater prevalence of digital learning since the Covid-19 pandemic. To a great extent, the University has been relying on the fact that most of the digital learning on campus has taken place in online courses developed in partnership with CEL. Partnership with CEL ensured compliance with this framework as a matter of course. Since digital learning materials are increasingly being developed without CEL partnership, it is important that the framework be made explicit. The framework should apply to all internally developed digital learning materials. Being explicit about them opens up greater opportunities for the continued expansion of digital learning on campus, including:

- expanded use of digital resources in all courses;
- potential for a greater variety of course delivery modes than before the Covid-19 pandemic, including current initiatives to expand the use of blended learning; and
- potential for more independently (instructor) created online and blended courses being created with ad hoc or no CEL support, while still assuring adherence to the articulated principles.

Next Steps:

This item is being submitted to the 21 November 2022 Senate agenda subject to SGRC endorsement on 14 November 2022. If SGRC does not endorse the framework, or if it proposes substantive changes thereon (which will require reconsideration at SUC), Senate will be so advised.

Documentation Provided:

- Digital Learning Principles and Guidelines

Universal Principles for Digital Learning¹

1. Learning materials and delivery platforms must conform to all relevant University policies, including meeting security, privacy, ancillary fee, and course outline requirements.
2. Platforms and materials must meet or exceed Accessibility for Ontarians Disability Act (AODA) requirements.
3. Learning materials must conform to Canadian Copyright law and UW Copyright guidelines.
4. Learning materials are subject to Policy 73 (see brief <https://uwaterloo.ca/associate-vice-president-academic/remote-teaching-and-learning-intellectual-property>) unless covered by separate development agreement or licensing (e.g., Creative Commons or Ontario Open License).
5. Waterloo encourages the reuse of digital materials created at Waterloo as well as the use of open educational materials (OERs) developed elsewhere, in an effort to reduce costs to the institution and to students.
6. Instruction should make use of university-supported platforms that provide adequate instructor and student support and ensure a more consistent teaching and learning experience.

Principles for an ONLINE class:²

1. is indicated in the schedule as “ONLN” and uses the appropriate components and scheduling.
2. can be completed remotely via digital delivery and does not require in-person activity or on-campus presence, except for in-person final exams (which may be supported in the student’s geographic location), although some online programs may have a short on-campus requirement (e.g., orientation session or capstone).
3. has the approval of the Dean or delegate (as determined in each Faculty), or Vice-President Academic & Dean (VPAD), and undergoes appropriate process to ensure quality and compliance with above principles before offer.
4. is recognized as equivalent to all other offers of the same course in terms of course credit, learning outcomes, and academic rigor.³
5. involves instructor effort equivalent to all other modalities.^{3, 4}
6. provides regular and timely access to instructors, as well as opportunities for meaningful interaction with instructors, other students, and content.
7. has a schedule that conforms to the academic calendar for the term including start and finish dates and any study breaks, and provides milestones and due dates for activities, assignments, and assessments.
8. uses the appropriate modality (asynchronous or synchronous) for the course content and learning outcomes, with consideration of the needs of the prospective/intended students. Waterloo encourages asynchronous delivery as it offers the greatest flexibility and access, among other benefits.

¹ “Universal” includes on-campus, blended, and online modalities.

² “Class” is intentionally used here as it denotes a specific offer and section of a course (i.e., there may be other sections or classes of the same course offered in different modes).

³ Online principles 4 and 5 were established by the UW Online Learning Task Force, 2008.

⁴ This principle supposes that modalities should be considered equivalent in terms of instructor workload.

Guidelines for Specific Online Modes

An asynchronous ONLN class:

1. has no scheduled meets.
2. may include *limited* synchronous elements, for which equivalent alternatives or flexible options exist.
3. has key content elements prepared sufficiently in advance of the course offer to facilitate a quality review, as well as ensure that students have timely access to necessary content during the course.
4. is developed either with the full assistance of CEL through the regular intake process *OR* undergoes an alternative process (see below) to ensure compliance with these guidelines and the academic standards of the Faculty that will offer the course before offer and receives final approval by Dean/VPAD (or delegate) before being scheduled.
5. features regular and substantive interaction, including access to instructors and meaningful interaction among students and instructors.⁵

A synchronous⁶ ONLN class:

1. has regular (usually weekly) scheduled online meets throughout term posted in Quest.
2. provides an alternative for students who cannot attend individual classes (e.g., recording of lectures).
3. has a course design and delivery plan that is reviewed by the Centre for Extended Learning (CEL).
4. is approved by Dean/VPAD (or delegate) before scheduling.

⁵ For reference, the phrase “regular and substantive interaction” is used in the U.S. to delineate between “distance education” and “correspondence education” for the purposes of establishing eligibility for federal aid.

⁶ i.e., a live class facilitated in real time using a tool like Zoom or Teams. This pre-supposes that synchronous online delivery will be a common ongoing strategy; the pending Digital Learning Strategy findings and recommendations may have a bearing on that.

Review and Approval of ONLN Courses developed outside of CEL process

Online courses developed outside the full CEL intake and development process (either with Agile Development Team assistance or fully instructor developed)⁷ would follow the following approval steps:

1. Dean/VPAD (or delegate) approves request for new ONLN course.
2. Author requests review by CEL. Timing should allow for review to be completed and approved by Dean/VPAD *before* course is scheduled for offer.
3. CEL reviews final course design using a checklist based on above principles, with the following possible outcomes:
 - a. Recommend
 - b. Recommend, with minor issues that can be quickly/easily rectified without additional review, or
 - c. Course has serious issues which must be addressed before offer and may require support and review (return to step 2).
4. In addition to CEL review, the Faculty or Affiliated and Federated Institutions of Waterloo (AFIW) may elect to conduct a peer review of content and course design.
5. Dean/VPAD (or delegate) issues final approval based on review(s).
6. A subsequent review or expiry date should be set for the course.

Questions and Implications

- Review and approval process really pushes the timeline forward for course creation.
- Diverging from historical practices (that most online courses were created and maintained with CEL assistance) removes the quality and subsequent oversight of above standards.
- should there be periodic review of these courses to ensure they meet standards in subsequent offers??
- Should Faculty, Dept, or program engage with CEL to review courses at regular intervals (e.g., like program reviews)?
- Should peer review be employed?
- CEL will have to create a Quality Checklist/resource package and also support reviews in a timely fashion

⁷ Currently, there is no policy requiring CEL support or approval for any modality.



MEMORANDUM

To: Senate Graduate & Research Council

CC: Bernard Duncker, Associate Vice-President, Research and International
Kathy Winter, Assistant University Secretary and Privacy Officer

From: Charmaine B. Dean, Vice-President, Research & International

Date: November 1, 2022

Subject: Renewal for Cybersecurity and Privacy Institute (CPI)

A handwritten signature in black ink, appearing to read "CBD", positioned to the right of the "From:" line.

- For decision -

Please see attached a proposal for the renewal of the Cybersecurity and Privacy Institute (CPI).

I am recommending that Senate Graduate and Research Council review this proposal, discuss, and vote on the renewal of the Cybersecurity and Privacy Institute (CPI).

27 October 2022

Dr. Charmaine Dean
Vice President, Research & International
University of Waterloo
200 University Avenue West
Waterloo, ON N2L 3G1

Cc: Dr. Bernard Duncker, Associate Vice President, Research & International
Senate Graduate and Research Council
University of Waterloo Senate

Dear Dr. Dean:

The Cybersecurity and Privacy Institute (CPI) was established by the University of Waterloo in 2018. Please accept this letter and the enclosed package as a formal request for the renewal of CPI for another five-year term.

CPI's goal is to build on the existing strengths of the University of Waterloo and significantly broaden the University's strength, reputation, and impact in cybersecurity and privacy. Since its establishment, CPI has undertaken a variety of initiatives to this end (Chapters 4-5 of the enclosed *Progress and Renewal Report 2022*). CPI has performed well in the strategic goals and objectives set in 2018 (Section 6.1). The enclosed report includes letters of support from Deans, the heads of other centers/institutes that closely collaborate with CPI, as well as from CPI members themselves (Appendices E-F). The most notable achievement of CPI is the leadership role it played in the formation of the National Cybersecurity Consortium (NCC) and the NCC subsequently being named as the lead recipient for an \$80-million grant by Industry, Science, and Economic Development (ISED) Canada for their Cyber Security Innovation Network (CSIN) program (Section 4.2). To quote from the letter of support for CPI by the current Managing Director of NCC, "*It is no exaggeration to say that without CPI, the University of Waterloo could not have played such an impactful role in NCC so far. Moreover, CPI will remain a reliable and essential partner for the future success of NCC and its sustainability*".

For the next five-year period, CPI has consulted extensively with its membership base and stakeholders to put forward seven strategic directions and initiatives (Chapter 6), focusing on building a sense of community within CPI's membership base, facilitating CPI members to (a) excel in research, (b) engage with other University units to respond to the critical talent gap in the cybersecurity and privacy domain, (c) nurture and leverage NCC, (d) make constructive contributions to public policy governing cybersecurity and privacy, and to strengthen and expand CPI's partnerships with industry and other stakeholders. The renewal of CPI will allow



us to see these initiatives through to fruition.

The enclosed *Progress & Renewal Report 2022* meets the requirements of the enclosed *Centres and Institutes Renewal Checklist* which has been annotated to pinpoint the Sections and Chapters that correspond to each item in the *Checklist*.

We at CPI greatly appreciate the support and encouragement you and your office have provided CPI since its inception, especially in paving the way for CPI to continue playing its essential and successful role in NCC. We thank you for your continued support in shepherding this request through to the Senate Graduate and Research Council and the University of Waterloo Senate for review and approval.

The *Guidelines for the Review of Centres/Institutes* require us to name “individuals who could provide external assessment of the Centre/Institute”. We submit the following names for your consideration:

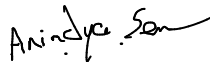
1. Paul van Oorschot (Carleton, FRSC, a University of Waterloo alumnus and the foremost senior cybersecurity academic in the country)
2. Benoit Dupont (UdeM, a criminologist who can bring in a social science perspective)
3. Ali Ghorbani (UNB, who directs Canadian Institute for Cybersecurity, the oldest university cybersecurity center in Canada, and the Managing Director of NCC)

These three individuals all hold CRC Tier-1 chairs and are widely respected cybersecurity and privacy experts in Canada.

Sincerely,



N. Asokan
Executive Director, CPI



Anindya Sen
Associate Director, CPI



Colin Russell
Managing Director, CPI

Enclosures (3):

1. Cybersecurity & Privacy Institute: Progress & Renewal Report 2022
2. (Annotated) Centres and Institutes Renewal Checklist
3. Presentation on CPI



CYBERSECURITY & PRIVACY INSTITUTE PROGRESS & RENEWAL REPORT 2022



CYBERSECURITY
AND **PRIVACY** INSTITUTE
UNIVERSITY OF WATERLOO

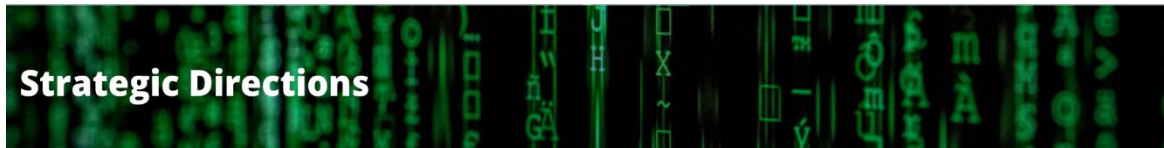


UNIVERSITY OF
WATERLOO

Contents

1	Introduction	5
1.1	Global Cybersecurity and Privacy Risks	5
1.2	Cybersecurity/privacy Talent Gap	6
1.3	Cybersecurity and Privacy Institute	6
2	Vision, Mission, and Goals	9
3	Scientific Directions	10
4	Achievements	13
4.1	Scientific Achievements	13
4.1.1	<i>Research Impact</i>	13
4.1.2	<i>Dissemination Impact</i>	16
4.1.3	<i>Policy Impact</i>	17
4.2	NCC	18
4.3	Grants & Partnerships	19
4.3.1	<i>External Research Collaborations</i>	20
4.3.2	<i>Institutional-level Applications for Major Provincial and National Grants</i>	21
4.4	Faculty Engagement	21
4.5	Student Engagement	24
4.6	Community Engagement – General Public	25
4.7	Supporting Community Events	26
5	Member Engagement	27
5.1	Online Engagement	27

5.2	Membership Survey	27
5.3	CPI’s Response to Feedback	28



Strategic Directions

6		29
6.1	Status of 2018 Strategic Plan Goals & Objectives	29
6.2	Alignment with UWaterloo’s Strategic Priorities	30
6.3	Strategic Directions (2022 to 2027)	32
6.3.1	Summary of Faculty Survey	32
6.3.2	Strategic Directions & Initiatives 2022 to 2027	32
6.3.3	Strategic Directions & Initiatives 2022 to 2027 – Expanded Detail	34



Activities and Services

7		39
7.1	Research	39
7.1.1	Research Support Services	40
7.1.2	Chippie Cluster – Compute Resources	40
7.1.3	Seed Grant Program	40
7.2	Training	44
7.2.1	University Courses	44
7.2.2	Professional Upskilling and Reskilling	44
7.2.3	Scholarships & Awards	45
7.3	Communications	45



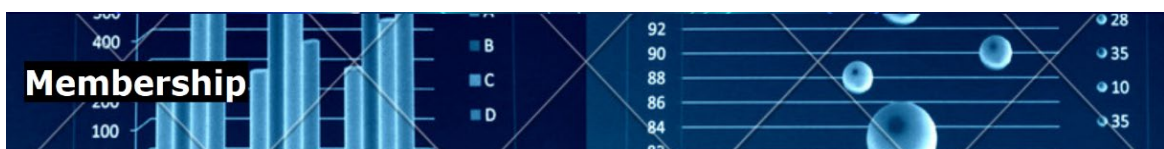
Governance

8		47
8.1	Structure	47
8.2	Reporting Structure & Board Composition	48
8.3	Current Board Members	48



EDI-R Mission Statement

9		49
---	--	----



Membership

10		50
----	--	----

10.1	Membership Categories	50
10.2	Faculty Members	51
11	Financials	54
11.1	CPI’s Initial Budget (2018)	54
11.2	Proposed 5-year Budget Plan for CPI	54
11.3	Budget Explanation	55
11.3.1	Salary Expenses	55
11.3.2	Office Expenses	56
11.3.3	Program Expenses	56
11.3.4	Steady State Budget Beyond 2027	56
12	Conclusions	58
13	Appendices	59
Appendix A	Membership Visuals	59
Appendix B	National Cybersecurity Consortium	62
Appendix C	Membership Survey	68
Appendix D	Policy Facing Achievements	69
Appendix E	Early Career Researchers - Support Letters	71
Appendix F	Support Letters	78
Appendix G	CPI’s Expertise Areas	106



Executive Summary

The Cybersecurity and Privacy Institute (CPI) was established in 2018 to facilitate collaborative research and training in cybersecurity and privacy. Through this direction, CPI's mandate provided opportunities for collaborations across the entire University and with companies, research centres, and other institutions in Canada and internationally.

CPI has provided strong and unique value to the University of Waterloo and its researchers. It has been integral to fostering interdisciplinary research collaborations and increasing the visibility and strength of UWaterloo's cybersecurity and privacy research to attract the best new faculty and to train world-leading talent. CPI has continued to grow, counting nearly 60 diverse faculty members, representing 16 departments and schools across all faculties, and has contributed significantly to a leadership role in the formation of the National Cybersecurity Consortium (NCC). Indeed, CPI researchers are seen as leaders in cybersecurity and privacy research, both domestically and internationally.

Over the past four years CPI has fostered world leading research, cybersecurity and privacy knowledge translation and mobilization, and contributed to improved policy for Canada. Through this lens CPI is proud to support its researchers with our Seed Grant program (Section 7.1.3), which has dispensed over \$225,000 to 12 different projects since its inception in 2018. Student support, alongside our industry sponsors, includes our scholarship program (Section 7.2.3), which has disbursed over \$50,000 to UWaterloo students. Furthermore, CPI has greatly expanded its communications, networking, and outreach endeavours. CPI continues to develop and promote its knowledge mobilisation and media presence, counting [CPI Talks](#), [CPI Spotlight Series](#), & [CPI RoundTable Discussions](#), as well as profiles in [YouTube](#), [Twitter](#), and [LinkedIn](#) amongst its recent initiatives.

Currently, CPI is expanding its strategic directions for the period 2022 to 2027, utilizing a reflective and comprehensive process that continually engages all members to ensure that our researchers can contribute to their achievements and propose strategic directions, supports, and priorities for the future. CPI has identified seven key areas as strategic priorities for the next five years (Section 6.3.2): continuing development of its support systems for the benefit of CPI researchers (Section 6.3.3.1), nurturing the NCC (Section 6.3.3.2), actively pursuing new opportunities with a focus on research collaborations (Section 6.3.3.3), upskilling and education (Section 6.3.3.4), building and maintaining partnerships (Section 6.3.3.5), positively affecting policy change (Section 6.3.3.6), and enhancing public awareness of cybersecurity and privacy issues (Section 6.3.3.7).

These strategic priorities will help CPI build on its successes in facilitating world leading research (Section 4.1), with its leadership in creation of the NCC (Section 4.2), supporting research grants (Section 4.3), effectively engaging with all CPI stakeholders including faculty (Section 4.4), students (Section 4.5), and the community at large (Section 4.6), and supporting community events (Section 4.7).

CPI is uniquely suited to strongly represent UWaterloo in the global cybersecurity and privacy theatre. The renewal of CPI and the continued support of its mission to promote and support cybersecurity and privacy research, training, and raising awareness is a critical contribution to the University of Waterloo's current and emerging strategic goals – the University's [current strategic plan](#) and its [research strategy](#) prominently identify cybersecurity and privacy as priorities.. The wide range of sources who have graciously provided renewal support letters ([Appendix E](#) - [Appendix F](#)) for CPI substantiates both CPI's broad impacts and its strong engagement base.

1

Introduction

Growing dependency on digital systems over the last 20-30 years [has drastically shifted](#) how most societies function. The COVID-19-induced shift to remote work has [accelerated the adoption](#) of platforms and devices that allow sensitive data to be shared with third parties, including cloud service providers, data aggregators, application developers, along with other technology-related intermediaries. These systems, while powerful tools for data and processing, attach an additional layer of dependency on third parties. Remote work has also moved digital interactions from office networks to residential ones, which have a greater variety of connected devices with less protection against cyber intrusion.

In parallel, the appetite for capabilities predicated upon using multiple technologies working in concert--including artificial intelligence (AI), Internet of Things (IoT) enabled devices, edge computing, blockchain-based systems, and next generation communication networks--[is only growing](#). While these capabilities afford tremendous opportunities for businesses and societies to use technology in ways that can dramatically improve efficiency, quality, and productivity, these same capabilities may also expose users to elevated and more pernicious forms of digital and cyber risk.

Digitalization increasingly impacts all aspects of our lives, including all professions and industries. As society continues to migrate into the digital world, the threat of cybercrime looms large, routinely costing organizations tens, and often hundreds, of millions of dollars. The costs are not just financial; critical infrastructure, societal cohesion, and mental well-being are also in jeopardy. Incorporating cybersecurity and privacy enhancing policies in technologies from the inception of their design and development is no longer optional; it underpins the survival and stability of our economic systems, as well as the transparency, sustainability, and trust in our communication tools. It is a matter of national and international security, which impacts every level of civilization. Against this backdrop we identify two major challenges: global cybersecurity and privacy risks and the talent gap in cybersecurity/privacy.

1.1 Global Cybersecurity and Privacy Risks

Many systems have critical assurance requirements. Their failure may endanger human life and the environment (e.g., nuclear safety and control systems, healthcare facilities), do serious damage to major economic infrastructure (e.g., cash machines, stock markets, international banking, online payments systems), endanger personal privacy (e.g., medical record systems, payment systems, rideshare systems), undermine the viability of whole business sectors (e.g., prepayment utility meters, digital infrastructure), and facilitate crime (e.g., security systems and car alarms, cyber-theft). Security and safety are becoming ever more intertwined, as there is software in almost everything we acquire (e.g., SW as a medical device, AI in everything).

Recent global events, such as the [ProxyLogon](#) patching frenzy, the [Emotet Shutdown](#), the [WannaCry](#) ransomware debacle, the pernicious [Apache Log4J Vulnerability](#), or the [SolarWinds supply chain attack](#), highlight the damage and loss of public faith that can be caused by hostile actors in the global digital space. The most visible of these cyberthreats are those that take place through our critical infrastructure. Recent examples include the [Colonial Pipeline shutdown](#), and [Ireland's Health Service Executive](#), as well as many hospital servers, which left some systems offline for 10 days! Considerably closer to home for UWaterloo, the Waterloo Region District School Board is cancelling busses because they still haven't recovered from their [cyberattack](#), and as of Sep. 15, rideshare program Uber has suffered a [significant cybersecurity breach](#). These events are expected to be more common in the coming years due to the sheer volume of connected devices and associated data gathering. For instance, "[the total installed base of internet](#)

of things connected devices worldwide is projected to amount to 30.9 billion units by 2025, a sharp jump from the 13.8 billion units that existed in 2021”.

Rapid digitalization has been accompanied by relentless data collection driven by the enormous appetite for extracting useful insights from data. Recent developments have also shown how such data can be misused in a variety of ways ranging from infringing on the privacy of individuals to influencing democratic processes. Understanding the potential for misuse and developing effective mitigation strategies is an urgent societal need.

The reality is that our economic model exerts massive competitive pressure on companies to rapidly introduce products and services into markets. Consequently, we have installed strategic vulnerabilities into our digital ecosystem, "by allowing poorly coded or engineered commercial-off-the-shelf products to permeate and power every aspect of our connected society. These products and services are prepackaged with exploitable weaknesses and have become the soft underbelly of government systems, critical infrastructures, and services, as well as business and household operations". This has inadvertently engineered an easy path for cybercriminals, as we have connected everything we possibly can to the Internet.

1.2 Cybersecurity/privacy Talent Gap

Already-overtasked IT and cybersecurity professionals are under an increasing burden, not only because of the expansion of remote work but also due to the growing complexity of regulations for data and privacy, even though such regulations are critical to [ensuring public trust](#) in digital systems. There is an [undersupply of security/privacy professionals](#)—a gap of more than 3.5 million worldwide, 25 thousand plus in Canada alone—who can provide technology leadership, test and secure systems, and train people in digital hygiene.

Leaders must remain attentive to perennial concerns like cybercrime and ransomware attacks as well. At the organizational level, upskilling leaders on cybersecurity issues and elevating emerging risks to board-level conversations will strengthen resilience. In a deeply connected society, digital trust is the currency that facilitates future innovation and prosperity. Trustworthy technologies, in turn, represent the foundation on which the scaffolding of an equitable and cohesive society is built. Unless we act to improve digital trust with intentional and persistent trust-building initiatives, the digital world will continue to drift towards fragmentation and instability, and the promise of one of the most dynamic eras of human progress may be lost.

1.3 Cybersecurity and Privacy Institute

The University of Waterloo’s Cybersecurity and Privacy Institute (CPI) is confronting these two challenges as part of maintaining a leadership role, by building on UWaterloo’s longstanding expertise in computer science, engineering, mathematics, cryptography, and quantum computing, to create world-leading cybersecurity technologies, and by increasing interdisciplinary collaboration across all faculties. The impact of this research is already being felt around the globe; CPI’s vision is to be internationally recognized as a leading interdisciplinary research institute making significant impacts in improving cybersecurity and privacy.

[UWaterloo’s Strategic Research Plan](#) identifies and promotes research topics in cybersecurity, cryptography, and privacy, as well as a focus on attracting and retaining high-quality faculty, whilst fostering interdisciplinary collaboration through meaningful interactions and exchange of ideas across disciplinary boundaries.

UWaterloo has already established a string of successes in these areas. UWaterloo has built on its expertise in mathematics for a focus on cryptography and had its first commercial impact [finding a vulnerability](#) in a

discrete logarithm cryptosystem chip that HP intended to bring to market. Experts in Combinatorics and Optimization (C&O) and Electrical and Computer Engineering (ECE) focused on the use of elliptic curves for public key cryptosystems, and their interest in the robustness of classical cryptography in a world with available quantum computing was part of the attraction for the first quantum researchers at UWaterloo, who seeded the formation of the Institute for Quantum Computing.

In the past 10 years, newly recruited experts in Internet, data, systems, and mobile security/privacy have strengthened UWaterloo's expertise in cybersecurity and privacy. UWaterloo's privacy researchers have created and transferred technologies, such as Off-the-Record Messaging, adopted by creators of popular instant messaging applications. Over the past 10 years, UWaterloo researchers in cryptography, security, and privacy have achieved important advances that have attracted international attention and adoption, as we explain in greater detail in Section 4.1.

Collectively, UWaterloo researchers working on the technological aspects of cybersecurity and privacy are recognized as world leaders. For example, according to csrankings.org, UWaterloo ranks among the top-15 institutions in the world and is the [top institution in Canada, by far](#). Although UWaterloo has long had multiple pockets of excellence in cybersecurity and privacy, the formation of CPI in 2018 has allowed UWaterloo to marshal these diverse groups across disciplines to achieve the critical mass necessary for success in major initiatives. A prime example is the founding role CPI played in the formation of the [National Cybersecurity Consortium \(NCC\)](#) and its success in winning the competition to be named the Lead Recipient of the \$80 million [Cyber Security Innovation Network \(CSIN\)](#) initiative by [Innovation, Science and Economic Development \(ISED\)](#) Canada. The presence of CPI as the single common representative of UWaterloo's cybersecurity and privacy experts was crucial in paving the way for UWaterloo to play its significant leadership role as a founding partner of NCC. Furthermore, in their successful applications for major grants, including one for a Canada Research Chair, CPI members have referred to CPI and its influence as evidence of strong institutional support for their research.

CPI has spearheaded several new initiatives to support excellence in cybersecurity and privacy research and training at UWaterloo. For example, the [CPI Seed Grant program](#) (Section 7.1.3) has helped CPI researchers bootstrap 13 new interdisciplinary research initiatives to date. CPI has also facilitated and supported its members in applying for major institutional level grants (Section 4.3). The [CPI Excellence Graduate Scholarships](#) (Section 7.2.3) have incentivized top graduate students of CPI members with annual scholarships.

To build a sense of community among CPI members, CPI has instituted a robust framework for communications, networking, and outreach. CPI has held an annual conference and several thematic events since its inception. These have been recently augmented by a number of new initiatives including our public outreach lecture series [CPI Talks](#), with [CPI RoundTable Discussions](#) intended to bring together small groups of CPI members and external stakeholders for focussed discussions on matters of common interest, our [CPI Spotlight Series](#) regularly highlighting the achievements of CPI members, a public CPI newsletter and presence in various social networks, and several new avenues such as mailing lists for CPI members and their students.

CPI has provided strong and unique value to the University of Waterloo and its researchers and has been integral to fostering interdisciplinary research collaborations and increasing the visibility and strength of UWaterloo's cybersecurity and privacy research to attract the best new faculty and to train world-leading talent. CPI has continued to grow, counting 60 diverse faculty members representing 16 departments and schools across all faculties. Indeed, CPI has established itself as a leader in cybersecurity and privacy research, both domestically and internationally.

To continue building on this strong foundation, CPI is seeking a renewal for the next five-year period. Based on broad consultations with members, CPI has identified seven key strategic priorities for the next five years (Section 6.3.2). The rest of this document lays out the achievements of CPI since its inception (Chapter 4) and plans for the future (Chapter 6). CPI is uniquely suited to strongly represent UWaterloo in the global cybersecurity and privacy theatre. The renewal of CPI and the continued support of its mission to promote and support cybersecurity and privacy research, training, and raising awareness is a critical contribution to the University of Waterloo's current and emerging strategic goals. The wide range of sources who have graciously provided renewal support letters (Appendix E - Appendix F) for CPI substantiates both CPI's broad impacts and strong engagement base.

2

Vision, Mission, and Goals

Vision - To significantly broaden Waterloo's strength, reputation, and impact in cybersecurity and privacy.

Mission - To facilitate collaborative research, training, and commercialization initiatives in cybersecurity and privacy, across the entire University of Waterloo community and in conjunction with industry partners, research centres, as well as provincial and federal governmental bodies, both in Canada and internationally.

Goals:

Knowledge Mobilization– To promote initiatives that will bring research to practical applications by maintaining a leadership role in working with industry and stakeholders to develop solutions, technologies, and education.

Research - To strengthen existing research collaborations among departments, schools, and faculties, and foster new collaborations, and to broaden the research and impact of UWaterloo researchers in all topics related to cybersecurity and privacy.

Equity, Diversity, Inclusivity, & Anti-Racism (EDI-R) - To remain committed to improving, expanding, and supporting the ongoing development and understanding of the issues related to equity, diversity, and inclusion, both within CPI and in those entities it engages with.

Education - To support and promote innovative and leading-edge cybersecurity and privacy training for students as well as the workforce.

Grants - To facilitate institutional-level applications for major provincial and national grants such as CFI, ORF, CERC, CFREF, CRC, and other grants, and to build on UWaterloo's long-term strength and more recent growth in the research and application of cybersecurity and privacy.

Brand - To increase the visibility and strength of UWaterloo's cybersecurity and privacy expertise to attract the best new faculty and HQP.

3

Scientific Directions

Within this chapter we discuss the scientific directions of CPI. CPI members strive towards the stated vision, mission, and goals by working across a broad front of cybersecurity and privacy topics. When CPI was founded, four CPI areas of expertise were identified (security, privacy, cryptography, quantum-safe communications). As the initial list was too coarse-grained, we initiated an exercise to refine and revamp the list, with input from CPI members. We began with a draft list and solicited feedback from several senior CPI members, as well as the members of the CPI Faculty Advisory Committee which has representation from every faculty. The revised list identifies the following nine primary areas of expertise:



Cryptography



Data Science - Security and Privacy



Human & Societal Aspects of Security and Privacy



Legal and Policy Aspects of Security and Privacy



Network Security



Operational Security



Privacy-Enhancing Technologies



Quantum-Safe Communication



Software, Hardware, and Systems Security

The list is intended to be descriptive rather than prescriptive and is used to find the right experts whenever an external partner approaches CPI with a request for proficiency. These nine areas are also indicative of the importance CPI places on addressing global cybersecurity risks, as they encompass a comprehensive and interconnected approach to understanding and proactively addressing the spectrum of cybersecurity and privacy concerns of the global community. Additionally, these areas of expertise expand on the specific fields within which the cybersecurity talent gap exists; illustrating the wide range of interdisciplinary skills required to effectively engage with multi-layered cybersecurity and privacy issues, e.g., implementing surveillance technology in the workplace requires hardware, software, legal, public relations, and ethics skillsets to be effective and responsible.

Figure 3-1 Ch.3 - *CPI Expertise Areas in Context* illustrates the interconnected nature of the nine expertise areas, in context.

Figure 3-1 Ch.3 - *CPI Expertise Areas in Context*

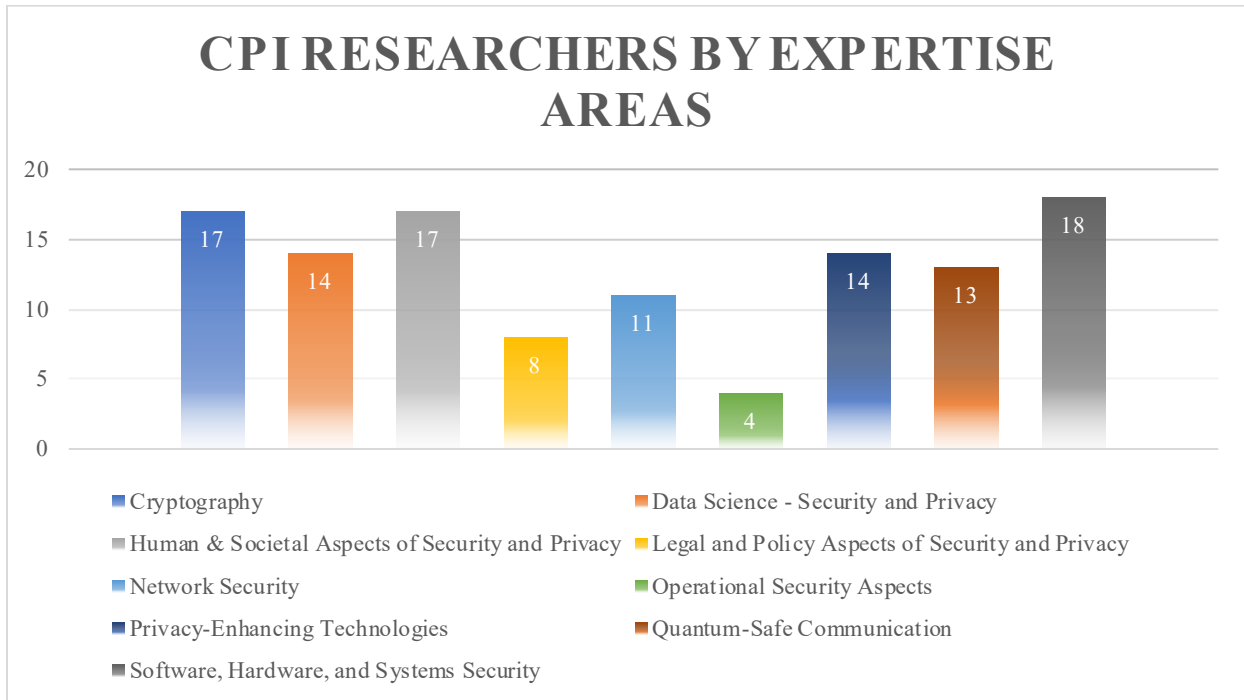


Software, Hardware, and Systems Security form the basis of any software/hardware implementation of cybersecurity and privacy systems (tools, services, applications etc.). **Privacy-enhancing Technologies** and **Cryptography** provide the basic building blocks that these systems can use. These building blocks can be used to build a more complex and purpose-specific suite of techniques for various needs, such as **Data Science Security and Privacy**. **Operational Security** is a cross-cutting concern that deals with the security and privacy issues in running computer systems.

Computer systems use network communications to interact with one another. **Network Security** seeks to understand and address the security concerns that arise from such interaction. **Quantum-safe Communications** is focussed on developing cryptographic mechanisms that are robust against quantum computers as well as on developing enhanced cybersecurity and privacy protocols by leveraging quantum mechanics. Computer systems also interact with people and with society as a whole. **Social and Human Aspects of Security and Privacy** involves understanding the security and privacy implications of individual and group behaviours in relation to technology. **Legal and Policy Aspects of Security and Privacy** deals with the intersections of law, cybersecurity and privacy, and policy implications of such interactions.

Figure 3-2 Ch.3 - *CPI Researchers by Expertise Areas* details researcher alignment within the expertise areas; Section 10.2 presents the list of CPI members and the expertise areas they identify with. CPI members volunteered to serve as the “designated area leads” for each of the expertise areas. The designated leads, in conjunction with all CPI members interested in specific expertise areas, helped formulate the characterization of each expertise area presented above and to identify examples of significant impact and achievements in each area (Section 4.1).

Figure 3-2 Ch.3 - CPI Researchers by Expertise Areas



4

Achievements

In this chapter, we highlight a sample of significant achievements by CPI and its members during the 2018-2022 period. This is not an exhaustive list. Where applicable, we refer to more detailed lists of achievements that appear in [Appendix B](#) & [Appendix D](#). We begin by describing the scientific achievements of CPI members. We then expand on the role that CPI has played in the formation of the NCC and its success thus far, as well as detailing Grants & Partnerships that CPI has contributed to. Finally, we outline CPI's record in engaging with various stakeholders (faculty, students, and the general public) as well as supporting community events.

4.1 Scientific Achievements



We begin with highlights of scientific achievements. Designated area leads, engaging with CPI members working in their particular area, produced detailed lists of achievements. In this section, we showcase a few examples from these lists, grouped into three categories: research impact, dissemination impact, and policy impact. The achievements listed in this section are intended to highlight the breadth and depth of the impact resulting from the work of CPI members and their students. CPI's role, via its initiatives and activities like those listed in [Chapter 7](#), is to facilitate an environment wherein CPI members can continue and expand their impactful achievements.

4.1.1 Research Impact

We describe examples of research impacts including projects that led to significant publications and knowledge transfer/mobilization.


United States National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardization Project: FrodoKEM Submission

Douglas Stebila (MATH/C&O) is a co-author of the [FrodoKEM](#) protocol, which was one of 69 proposals submitted to the NIST post-quantum cryptography standardization project in 2017. Over the past 4 years, FrodoKEM has advanced through the review process and in 2020 advanced to Round 3 of the project as one of five alternate candidates. In December 2019, the German Federal Office for Information Security began recommending FrodoKEM as one of two algorithms suitable for post-quantum security and continues to recommend FrodoKEM in their annual recommendations.

Expertise areas:  

WAGE: An Authenticated Encryption with a Twist

Designing a lightweight cryptographic primitive requires a comprehensive holistic approach. Guang Gong (ENG/ECE) et. al. have developed [WAGE](#), a new lightweight sponge-based authenticated cipher based on the well analyzed Welsch-Gong Permutation (co-developed by Guang Gong and designed for lightweight cryptography). The performance of WAGE balances the tension between hardware efficiency and a good security guarantee. WAGE was a round 2 candidate of the NIST lightweight cryptography competition.

Expertise areas: 

Palitronica

[Palitronica](#) is a Canadian company formed in 2019, with Sebastian Fischmeister (ENG/ECE) as its CEO. Their mission is to protect critical infrastructure and key resources from cyberthreats. Energy, communications, transportation, healthcare, and other sectors are under constant attack from adversaries including nation states, cybercrime gangs, and malicious insiders; Palitronica builds and deploys cutting-edge solutions to defend critical infrastructure and key resources, through their products:


- **Palisade** - adds cyber-protection to established critical systems without the need for recertification. Palisade detects hardware and software tampering and can detect ransomware attacks in infrastructure before they reach a critical point.
- **Anvil** - verifies the integrity of products before they are deployed to customers, facilitating the rapid detection of implants, modifications, and weaknesses introduced through manufacturing and sourcing. Anvil acts as a shield between products and their supply chain, preventing unsolicited modification to products and elevating customer trust and confidence.

In Dec. 2021 they were accepted to the [Y Combinator](#), an American technology start-up accelerator. With a 1.5% acceptance rate, it's considered to be one of the most renowned start-up accelerators in the world, and has backed over 3000 companies such as Airbnb, Stripe, Dropbox, Coinbase and Reddit. As of Jan. 2021, the combined valuation of the top YC companies totals more than \$300 billion.

Expertise areas: 


NSERC/RBC Chair in Data Security

The founding executive director of CPI, Florian Kerschbaum (MATH/CS), was able to intensify the relation with Royal Bank of Canada and secure an industrial research chair, the [NSERC-RBC Industrial Research Chair in Data Security](#). The chair's research agenda works in close alignment with RBC's data analytics team and aims to address their privacy challenges. RBC is Canada's largest bank, and they are committed to protecting the privacy of its customers. Florian Kerschbaum's team develops solutions that enhance the privacy of RBC's data analytics practice.

Expertise areas: 


Paternalistic Surveillance as a Mode of Carceral Expansion

Jennifer Whitson (ARTS/SOC & LS) and her graduate student Krystle Shore have been focusing on public health surveillance and its intersection with routine policing practices. Consumer-facing tracking devices are marketed both to police agencies and caregivers of those with Alzheimer's and dementia, allowing both parties to track the movement and habits of their adult wearers. They illustrate how these technologies and services are framed by marketers as a silver bullet solution for aging populations amidst eroded social support networks, but fundamentally operate as coercive and highly commercialized surveillance under a veneer of protection. Vulnerable adults enrolled in the tracking programs by their caregivers become part of a carceral expansion, where data on their movements and habits are shared with first responders and policing agencies. Knowledge of these practices allow the public and regulators to understand the nuances of surveillance and make decisions that balance security and privacy.

Expertise areas: 


CANARIE Joint Security Project

The security of our digital resources, and the infrastructures that support them, are of paramount importance to Canadians, especially Canada's research, education, and innovation communities. The CANARIE Joint Security Project is a community driven approach to addressing the security of these institutions. Raouf Boutaba (MATH/CS) et. al. developed the [UWaterloo Intrusion Detection System](#) platform, a data aggregation and analysis hub that ingests more than 1TB of connection data per day from 79 Canadian institutions. It uses both machine learning and graph-based methods, as well as threat feeds, e.g., CanSSOC feeds, to detect threats. The platform provides dashboards and notebooks to visualize and investigate threats and allows sharing of threat intelligence with participating institutions.

Expertise area: 

PUPy





In modern life, the usage of smart devices like smartphones and laptops that allow for access to information, communication with friends and colleagues, and other indispensable services, has become ubiquitous. All modern smart devices employ some form of authentication to ensure that access to this confidential data by the wrong person is avoided. This authentication method is usually some form of explicit authentication, which can be detrimental to the user's experience, often leading to users forgoing authentication entirely. Implicit authentication aims to limit the number of explicit authentications that are necessary for the user, using passive approaches to authenticate the user instead. Context detection frameworks aim to reduce explicit authentications by disabling explicit authentication entirely, when appropriate. [PUPy](#), created by Urs Hengartner (MATH/CS) and his student Mathew Rafuse, is an open-source context detection framework that can be used for building context-dependent authentication solutions. It provides a large amount of context information through a simple interface, by taking in sensor data and condensing it into three values - privacy, unfamiliarity, and proximity: privacy tracks the privacy of the current context; unfamiliarity tracks how many unfamiliar people are around; and proximity estimates the distance between the device and the user.

Expertise area: 

Improving Privacy-preserving Communications Networks

Privacy-preserving communications networks allow people to communicate with each other, and to access online information, without automatically revealing personal information, such as their Internet addresses. The largest such network is The Onion Router (Tor). Ian Goldberg (MATH/CS) and his group have contributed significantly to the Tor platform, including the following:


- [PIR for Onion Services](#)
Private Information Retrieval for Onion Services is a prototype implementation of Tor with support for asynchronous PIR lookups for onion services. Such private lookups prevent malicious Tor onion service directories from learning the relative popularity of onion services or breaking the unlinkability guarantees of Tor's v3 onion service addresses
- [ConsenSGX](#)
ConsenSGX is their work on using trusted execution environments such as Intel SGX to allow Tor clients to fetch only small parts of the Tor network consensus document, without opening them up to epistemic attacks
- [Website Fingerprinting](#)
Website fingerprinting is a classification attack wherein someone watching a user's local network can determine what websites they are visiting, even if they are using privacy enhancing technologies such as encryption, VPNs, or Tor. The group has implementations of old and new website fingerprinting attacks and defenses
- [NetMirage](#)
NetMirage is a tool for testing IP-based networked applications. NetMirage emulates a large virtual network, allowing you to run and test unmodified applications in real-time. It is compatible with any IP-based Linux application with the capability to bind to a specific IP address. In particular, NetMirage is a modern tool for constructing large-scale virtual Tor networks

Expertise areas:    

Hardware-assisted Runtime Protection



Runtime attacks, which involve attacking a program while it is running by exploiting memory vulnerabilities, are endemic. They have featured in most major attacks in the last three decades. While several protection mechanisms have been proposed and implemented, they involve a trade-off between cost of protection and effectiveness. In this project, N. Asokan (MATH/CS) et. al. explored how this trade-off

can be avoided by making use of hardware assistance. Their work has been funded by NSERC as well as several major industry players, including Intel and Google, resulting in significant [top-tier](#) publications.

Expertise area: 


Android SmartTVs Vulnerability Discovery via Log-Guided Fuzzing

The recent rise of Smart IoT devices has opened new doors for cyber criminals to achieve negative outcomes unique to the ecosystem. SmartTVs, the most widely adopted home-based IoT devices, are no exception. To proactively address the problem, Yousra Aafer (MATH/CS) et. al. proposed a [systematic evaluation of Android SmartTVs security](#). They overcame a number of prominent challenges, such as most of the added TV related functionalities are (partially) implemented in the native layer and many security problems only manifest themselves on the physical aspect without causing any misbehaviors inside the OS. They developed a novel dynamic fuzzing approach, which features an on-the-fly log-based input specification derivation and feedback collection.

Expertise areas:  

Axelar

Sergey Gorbunov (MATH/CS) is a founder of [Axelar](#), a spin-out from his lab. Axelar is a scalable cross-chain communication platform universal overlay network, securely connecting all blockchain ecosystems, applications, assets, and users to deliver Web3 interoperability. Axelar is composed of a decentralized network of validators, secure gateway contracts, uniform translation, routing architecture, and a suite of software development kits (SDKs) and application programming interfaces (APIs) to enable composability between blockchains. This allows developers to build on the best platform for their use case, while being able to access users, assets, and applications in every other ecosystem. Instead of pairwise cross-chain bridges, they can rely on a network architecture that provides a uniform code base and governance structure. An exceedingly successful commercial entity, Axelar's latest Series B funding round has brought Axelar's valuation to \$1 billion USD.



Expertise area: 

4.1.2 Dissemination Impact

Here we describe examples of dissemination impacts including major open-source projects as well as books.

Open Quantum Safe Software Project

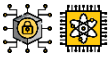
Douglas Stebila (MATH/C&O) and Michele Mosca (MATH/C&O) co-founded the [Open Quantum Safe \(OQS\)](#) project. The goal of the project is to develop open-source software for prototyping and evaluating quantum-resistant cryptography and, as of 2021, it is the largest open-source post-quantum cryptography software project in the world. One of the challenges to deploying reliable quantum-safe cryptography was the lack of a reliable open-source platform to support the development and prototyping of post-quantum cryptography. OQS plays an important role in the evaluation of the algorithms being considered for standardization, one of the most important milestones in the practical deployment of post-quantum cryptography. OQS has integrated its cryptography library, `liboqs`, into a fork of OpenSSL and OpenSSH, and external groups are increasingly using it; including Microsoft's Post-Quantum Cryptography VPN, Thales eSecurity, Go Wrapper, and Utimaco's Hardware Secure Module.

Expertise areas:  

OpenQKDSecurity


Norbert Lütkenhaus (SCI/PHYS & ASTRO) and Michele Mosca (MATH/C&O) developed an open-source platform for the numerical analysis of generic QKD protocols. The security analysis of QKD protocols is quite demanding for new researchers entering the field. The underlying mathematical problem is a convex

optimization problem. In the past, the majority of effort has been spent on solving those exactly using symmetries of protocols as basis of parameter reduction. The [OpenQKDSecurity](#) approach converts the problem into a form that can be solved efficiently for general protocols, including those that don't have symmetry. OpenQKDSecurity serves as a platform for interaction between different research communities (experimentalists, cryptographers, and mathematicians) that can work on those aspects that correspond to their respective strengths. The entry threshold for new researchers exploring improved protocols is therefore lowered.

Expertise areas: 


Differential Privacy for Databases

Xi He (MATH/CS) and her co-author Joseph P. Near published a [book](#) on differential privacy in the Foundations and Trends in Databases series. Differential privacy is a promising approach to formalizing privacy—that is, for writing down what privacy means as a mathematical equation. This book serves as an overview of the state-of-the-art in techniques for differential privacy. In particular, the authors focus on techniques for answering database-style queries, on useful algorithms and their applications, and on systems and tools that implement them. These techniques represent significant progress towards building differentially private database systems. The approaches described in this book have already resulted in useful, deployable systems, and likely pave the way towards increasingly widespread adoption of differential privacy in such systems.

Expertise areas: 

Hardware Platform Security for Mobile Devices

N. Asokan (MATH/CS) and his postdoctoral researcher Hans Liljestrand, along with their co-authors, published a [book](#) on hardware-assisted platform security mechanisms on mobile devices in the Foundations and Trends in Privacy and Security series. Hardware platform security mechanisms like hardware-assisted trusted execution environments are now widely deployed, especially on mobile devices like smartphones. At the same time, recent developments like transient execution attacks (the most well-known of this class of attacks are [Spectre](#) and [Meltdown](#)) have questioned the validity of relying on hardware security mechanisms as inviolable. This book traces the history of hardware platform security mechanisms, describes the state-of-the-art in both attacks and defenses, and outlines potential lines of future development. It is intended as a resource for students embarking on research in the area, as well as practitioners.

Expertise area: 



4.1.3 Policy Impact

We now describe initiatives geared towards influencing cybersecurity and privacy policy.

Understanding the Risks and Regulation of Workplace Surveillance in Canada's Digital Economy



In a post-COVID work from home environment, protection of individuals' privacy, security, as well as the separation of personal and professional lives from an employer's surveillance, is increasingly important. Employee monitoring technology is a \$14.5B industry, with significant potential for employer overreach and misuse. Adam Molnar (ARTS/SOC & LS) is leading a highly interdisciplinary and inter-sectoral inquiry involving a multi-pronged approach to the issues at hand, combining legal and sociological qualitative inquiry, in conjunction with hardware and software testing. This initiative provides i) policy recommendations for workplace privacy and cybersecurity both federally and provincially, ii) informing the legal / policy regulation of employee monitoring vendors, iii) software/design related changes that can be a part of these regulatory recommendations, and iv) partnerships with civil society groups such as the British Columbia General Employees' Union (BCGEU) and the Canadian Civil Liberties Association (CCLA). This initiative is expected to generate resources for the BCGEU that can assist them with

negotiating protocol on workplace surveillance and privacy, and with the CCLA on legal analysis and information that they can use on education and awareness on workplace privacy rights for Canadians.

Expertise areas:  

Canadian Forum for Digital Infrastructure Resilience Quantum Readiness Working Group

Michele Mosca (MATH/C&O) chairs the Canadian Forum for Digital Infrastructure Resilience (CFDIR) [Quantum Readiness Working Group](#). The CFDIR is a voluntary, consensus-based, and action-oriented public-private collaboration formed to enhance the resilience of the Canadian critical digital infrastructure and influence policy, resulting in a trusted digital economy for Canadians and a thriving cyber security industry. Innovation, Science, and Economic Development Canada (ISED) established CFDIR in 2020, in part to support Canada's National Strategy for Critical Infrastructure. Under this strategy, ISED is the lead federal department for the Information and Communication Technology critical infrastructure sector. CFDIR brings together key federal partners and industry to improve digital infrastructure resiliency.

Expertise areas:  

OHT Information Management Plan

Ian McKillop (HEALTH - MATH/CS) contributed to the development of security and privacy policies for one of Ontario's new Health Teams. This includes leading the data collection component of the research, holding workshops with affected stakeholders, analyzing findings, and generating a report of recommendations for a go-forward plan as Ontario engages in a strategy to promote the exchange of data between data custodians in a manner that complies with legislation and reflects best security practices whilst enabling seamless patient care.

Expertise area:  

4.2 NCC

In 2020, under the leadership of the previous executive director, Florian Kerschbaum, CPI along with four other major Canadian university-based cybersecurity centres and institutes formally established the National Cybersecurity Consortium (NCC) as a federally incorporated not-for-profit entity. The founding members of NCC were:

- **Cybersecurity and Privacy Institute**, University of Waterloo
- **Institute for Security, Privacy and Information Assurance**, University of Calgary
- **Centre for Cybersecurity**, Concordia University
- **Canadian Institute for Cybersecurity**, University of New Brunswick
- **Rogers Cybersecure Catalyst**, Toronto Metropolitan University

NCC was formed to bridge all cybersecurity expertise within Canada. The initial objectives of NCC were:

- Consolidate all cybersecurity and privacy related research expertise in Canada through one hub
- Facilitate academic, industry, government, and international collaborations
- Respond to government program and policy announcements and requests

In February of 2022, Innovation, Science, and Economic Development Canada, (ISED) announced that the NCC was chosen as the lead recipient for a \$80 million grant over four years to run the Cyber Security Innovation Network Program (CSIN). The CSIN program will ensure Canada is globally competitive and establishes a leadership role in cybersecurity allowing for the cyber-resilience of our critical infrastructure, the privacy and safety of citizens' data, improvement of policy, and the safety and assurance of our digital ecosystems. It is envisioned as a pan-Canadian network that will support the growth of Canada's cybersecurity ecosystem through industry and academia collaboration. CSIN will seek to enhance research

and development, increase commercialization, and further support the development of skilled cyber security talent across Canada and is tasked with the following objectives:

- support research and development in cyber security by encouraging collaboration between Canada's post-secondary institutions, the private sector, and other partners in order to accelerate the development of innovative cyber security products and/or services
- seek to accelerate the commercialization of cyber security products, services, and/or processes
- seek to diversify, deepen, and expand Canada's cyber security pipeline of talent, including the recruitment and retention of faculty, trainers, and instructors, and by providing more resources to curriculum development, training, reskilling, and upskilling of the cyber security workforce through initiatives designed and delivered in collaboration with industry partners

CPI Integral to NCC Success

Throughout late 2020 and 2021, CPI staff and the Office of Research at the University of Waterloo began to build the NCC's first private and not-for-profit sector memberships. Colin Russell, managing director of CPI and manager of corporate research partnerships of the office of research, worked closely with Krista Hrin, operations manager of CPI, and Florian Kerschbaum to begin a large outreach campaign. The inception of the outreach campaign by CPI pre-dated that of the other founding partners by over 8 months.

Marketing materials and outreach strategies were drafted and conceived by CPI that spoke to every sector of Canadian business. The goal was to not only draw attention to and membership in the NCC, but to also advocate for the importance of cybersecurity and privacy to all sectors of business. It quickly became apparent that the advocacy component of the outreach was to be a hallmark of conversations with businesses in many sectors.

The lessons learned throughout 2020 and 2021 were to inform how the other founding academic partners of the NCC would recruit further private and not-for-profit sector partners. Indeed, CPI was so far ahead of the other partners in private and not-for-profit sector recruitment that CPI's managing director, Colin Russell, was nominated to lead the business development committee of the NCC in 2021. Further, the marketing materials created in 2020 formed the basis for the committee's outreach.

By the time of submission to ISED's CSIN program the NCC grew from a small group of 5 academic institutes and centres to fielding a membership of 122 participating organizations across Canada, including:

- 42 post-secondary institutions – with a combined 140 researchers (*20% CPI members*)
- 46 companies
- 26 not-for-profit organizations
- 8 governments/governmental agencies

Private and not-for-profit sector members found value in the objectives of the NCC (i.e., R&D, Commercialization, and Training) and provided commitments to leverage funding in anticipation that ISED would award the CSIN program to NCC. Indeed, through the business development activities led by CPI, 78 proposals were identified as potential projects that can be implemented in the first year of operations, including 13 proposed shovel-ready projects by CPI members in training, commercialization, and research.

For more information on NCC, see [Appendix B](#).

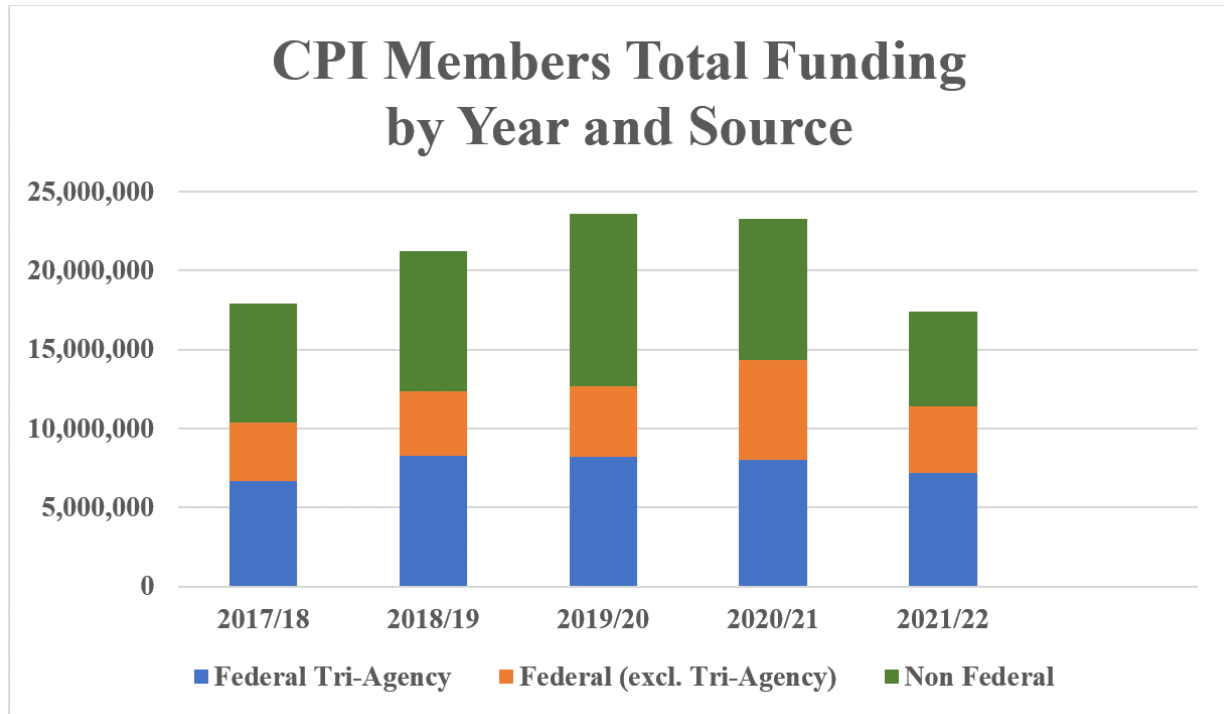
4.3 Grants & Partnerships

The establishment of CPI has assisted researchers by demonstrating the high-level of institutional support for cybersecurity and privacy research at UWaterloo. CPI has facilitated, directly and indirectly, the strengthening of institutional-level applications for major provincial and national grants, proposals for

chairs like CRC and NSERC Industrial chairs, and major industry engagement initiatives. CPI is predicated on supporting researchers through providing networking opportunities, grant and project facilitation, knowledge mobilization, and community building initiatives.

Figure 4-1 Ch.4 - *CPI Members Total Funding by Year and Source* illustrates funding obtained by CPI members during the past five years. CPI was formed in 2018.

Figure 4-1 Ch.4 - CPI Members Total Funding by Year and Source



*Total funded activity of all members of CPI, not necessarily indicative of exclusively CPI facilitated or cybersecurity and privacy specific research initiatives.

4.3.1 External Research Collaborations

CPI has supported many external collaborations and projects. The following are examples that were reported by CPI members when surveyed to share their significant achievements.

- Syncor sponsorship – 2019 Graduate Excellence Scholarship
- BlackBerry sponsorship via OR/GEDI collaboration agreement – 2020-2021 Graduate Excellence Scholarships
- Matching funding grants, leveraging industry funding
 - NSERC Alliance (BlackBerry: **Azad** ENG/SYDE)
 - NSERC Alliance (Crypto 4A Technologies: **Stebila** MATH/C&O, **Mosca** MATH/C&O, **Lütkenhaus** SCI/PHYS & ASTRO)
 - ORF-RE (Rogers: **Boutaba** MATH/CS)
 - ORF-RE (RBC: **Kerschbaum** MATH/CS, Intel: **Asokan** MATH/CS)
- RBC-NSERC Industrial Research Chair in Data Security (**Kerschbaum** MATH/CS)
- Magna-NSERC Industrial Chair in Automotive Software for Connected and Automated Vehicles (**Fischmeister** ENG/ECE)

- Public Works and Government Services Canada - Post-quantum cryptography research (**Stebila** MATH/C&O, **Jao** MATH/C&O, **Mosca** MATH/C&O)
- CPI member projects funded via the Data Trust strand in Huawei – UWaterloo Joint Research Lab
- Office of the Privacy Commissioner - Understanding and Responding to the Privacy and Security Risks of Stalkerware (**Molnar** ARTS/SOC & LS)
- CANARIE (**Boutaba** MATH/CS)
 - University of Waterloo Intrusion Detection System Extension
 - Joint Security Project – Data Aggregation & Visualization Tools
- DnD IDEaS/MINDS:
 - Mission-oriented cybersecurity and defence: SIVUS-2: Side-channel-based Vulnerability Scanner (**Fischmeister** ENG/ECE)
 - 5G Micronet - Secure and Reliable End-to-End Network Slicing for 5G and Beyond Mobile Networks (**Boutaba** MATH/CS, **Barradas** MATH/CS)
 - Defence and Security Foresight Group (**Momani** ARTS/PSCI, **Kitchen** ARTS/PSCI)

4.3.2 Institutional-level Applications for Major Provincial and National Grants

CPI has supported its members in their efforts related to institutional-level grants and funding. The following are some illustrative examples, as reported by CPI members.

- CFREF - Transforming Health Technologies proposal development (support **Adam Molnar's** (ARTS/SOC & LS) participation)
- CFI-IF/ORF-RI proposal - Understanding Privacy, Security, and Cryptography in Online and Physical Environments (**Goldberg** MATH/CS)
- Canada Research Chair in Privacy Enhancing Technologies (**Goldberg** MATH/CS)
- CPI members funded under the National Research Council (NRC) – University of Waterloo Collaboration Centre Funding Program (2022) (NUCC)
- NSERC SPG - Security and Privacy for Hybrid Centralized and Blockchain Computing in the Internet of Things (**Gong** ENG/ECE)
- SSHRC Partnership Grant - The Human-Centric Cybersecurity Partnership (**Molnar** ARTS/SOC & LS)

4.4 Faculty Engagement

CPI is predicated on a constant feedback cycle that creates iterative change, in order to best serve its membership base. In response to our [membership survey](#) ([Appendix C](#)) and individual feedback, CPI has a number of on-going and new initiatives intended to benefit faculty members. These include:

- **Seed Grant Program** – an initiative that CPI has been running for several years, with one or more calls for proposals each year, providing funding to assist CPI researchers in their efforts to incept new research initiatives, with a focus on encouraging interdisciplinary collaborative efforts. Our membership survey ([Appendix C](#)) indicated that CPI members particularly appreciated the Seed Grant Program (Section 7.1.3).
- **CPI Talks** – a public outreach lecture series launched in 2021. It features well-known experts speaking on cybersecurity and privacy topics that concern the general public as a whole. They are intended for people from all walks of life, and are designed to be accessible to anyone, without any background or knowledge in cybersecurity and privacy. They are also intended to provide a way for CPI experts themselves to better understand and appreciate the interdisciplinary considerations involved in cybersecurity and privacy challenges.
- **CPI RoundTable Discussions** – an interdisciplinary outreach discussion program launched in 2022 to bring CPI researchers interested in selected multidisciplinary topics to the same table in the hope of kickstarting potential collaborations. Our intent is to organize these events

in collaboration with other university institutes and centres and/or focussing on specific themes of interest to CPI researchers.

- **Communications Revamp** – a new communications strategy aimed at providing greater engagement with CPI faculty members consisting of (a) monthly Executive Director emails, (b) a new cpi-faculty mailing list, (c) a dedicated Microsoft Teams channel, and (d) an expansion of our efforts to engage with CPI members on multiple platforms to provide greater community and engagement.
- **Chippie Cluster** – a high-performance computing infrastructure with significant compute resources (Section 7.1.2) for CPI members and their students. It was first set up in 2021 based on a poll of CPI members regarding the kinds of computing resources deemed most useful to them. In 2022, we plan to augment the range of resources.
- **Faculty Advisory Committee** – a group of [faculty members](#) drawn from across all academic units at the university. The CPI leadership team and staff periodically engage with the members of the advisory committee to solicit advice and feedback regarding CPI operations and strategy.
- **CPI Spotlight Series** – are interview-based articles that highlight our researchers with their research and ideas in our regularly scheduled [Spotlight Series](#) on our public website.

Early Career Researchers:

An important contribution of CPI has been its impact on the research activities of early career scholars in the university. As noted elsewhere (Section 7.1.3) in this report, a significant number of grants from CPI's seed funding initiatives have gone to either assistant professors or recently promoted associate professors. Specifically, CPI has enabled like-minded researchers from different fields to build research capacity and produce innovative work, teaching, and public outreach activities. It is important to note that the impacts of CPI go beyond seed funding. For example, through its networks, CPI has been able to connect faculty to outside opportunities (Section 4.3.1). The following CPI members who are, or were, ECRs during the progress report period have provided support letters ([Appendix E](#)) outlining the positive impact CPI has made in their respective career trajectories.

- **Leah Zhang-Kennedy**, (ARTS/STRATFORD SID&B) Assistant Professor at the Stratford School of Interaction Design and Business, states that CPI has supported her with research funding, collaboration and networking opportunities, and supported knowledge mobilization initiatives, and notes that the contribution of CPI is threefold. First, the institute helped promote the importance of interdisciplinary collaboration in creating privacy solutions. Second, CPI funding provided valuable networking opportunities between the Stratford School and CPI's network of researchers, industry professionals, and entrepreneurs. Third, the funded event (uXperience) introduced many university students to cybersecurity and privacy as potential career paths.

Zhang- Kennedy has obtained two CPI seed funds:

- uXperience - Think Privacy Design Jam at the Stratford School of Interaction Design and Business - was funded by a CPI Seed Grant and brought together post-secondary students across diverse backgrounds such as interaction design, computer science, engineering, communications, and sociology and legal studies. This event encouraged students to explore, collaborate, and propose novel solutions that address the role and impact of design on people's privacy. Amongst other impacts, the Jam succeeded in introducing university students to cybersecurity and privacy as potential career paths and provided students from different backgrounds the opportunity to work together and find creative solutions to important problems
- Collaborative, Secure Software Development Software project - security is influenced by various actors beyond the software developer. This project proposes investigating

how interdisciplinary teams (e.g., developers, designers, engineers, security analysts) work collaboratively to design, develop, test, and maintain secure software. The project's objectives are to understand how practitioners collaborate on security-related tasks, explore methodologies and processes used that influence software security, and identify opportunities and barriers for effective secure software development in team-based environments

- **W. Alec Cram**, (ARTS/ACCT) Associate Professor at the School of Accounting and Finance, has benefited from CPI's connections with a provincial ministry that have resulted in a large research and consulting project with another CPI member - Ian McKillop - and an SAF doctoral student. This specific opportunity has the potential to result in several high-quality research publications. His view is that CPI provides a critical role as a central hub of cybersecurity activity at the University.
 - Over the past year, W. Alec Cram has been contacted by CPI in regard to several promising opportunities to connect with organizations that require cybersecurity expertise, as well as ongoing developments with cybersecurity teaching. In particular, he notes that the connection with practitioners is often difficult to come by, but CPI is in an ideal position to act as an intermediary to connect interested organizations with specialists at the University
- **Jennifer R. Whitson**, (ARTS/Soc. & LS – SIDB) Associate Professor Sociology and Legal Studies / Stratford School of Interaction Design and Business, notes that networks developed through CPI have made them a more skilled researcher, graduate supervisor, and instructor.
 - Jennifer Whitson highlights one of the most fulfilling parts of their early research career has been their collaborations with Ian Goldberg at the Cheriton School of Computer Science. The CPI Seed Grant for a conference (SANDPIT), was their first collaboration together. Speakers included Pulitzer-prize winning journalist Julia Angwin and Scott Millar, Deputy Chief, Policy and Communications at Communications Security Establishment (CSE). Along with a full slate of speakers, it hosted graduate student speaker talks and poster sessions. Five of the speaker talks may be viewed [here](#).
 - Without the initial funded collaboration, Ian Goldberg and Jennifer Whitson would likely not have taken the risk of [teaching together](#). SOC 701/CS 858 was the first co-taught course at Waterloo to be offered between Sociology and Legal and Studies and Computer Science. The course focused on Surveillance and Privacy Enhancing Technologies, and attracted students from Computer Science, Sociology, Political Science, Global Governance, English, Systems Design Engineering, and Applied Health Science, as well as faculty auditors in Optometry and Computer Science, which is strong evidence supporting CPI's commitment to promoting interdisciplinary engagement and collaboration
 - Jennifer Whitson also underlines another central role of CPI in providing resources and a network that assists their department in recruiting top talent, as Adam Molnar joined CPI immediately upon their arrival. The availability of seed grants and research collaborators from other faculties is valuable for both recruiting and helping faculty 'hit the ground running' as they join UWaterloo, and to help them build research capacity. Currently, their department has the greatest hub of surveillance studies researchers in Canada. CPI grants have also supported Whitson's graduate students, Brian Schram and Krystle Shore, and provided a venue for their work, both at the CPI Annual Conference and online. For example, CPI funded the creation of a video promoting grad student Brian Schram's dissertation project. This [video](#) was useful as public knowledge mobilization and was re-used by the Faculty of Arts in their social media recruiting
- **Meng Xu**, (MATH/CS) Assistant Professor at the Cheriton School of Computer Science, has been invited to three round-table discussions with both university institutions (RoboHub), and

industrial partners (BlackBerry & EPAM). Through these discussions, he has made the initial contact to many potential collaborators and was offered channels and support to apply for both CPI seed funding as well as external funding (e.g., from NSERC). Out of these discussions, at least one will mature into multi-year funding.

- Meng Xu highlights the Chippie cluster as meeting the parallelization requirement for his research work, and the annual poster session that provides an opportunity where he and his students can advertise their ongoing research and source for early feedback
- Meng Xu notes his view that CPI is determined to address the significant shortage of skilled cybersecurity professionals, referencing that he co-instructed CS458 - Computer Security and Privacy in the Winter 2022 term and that he co-piloted the first CPI Undergraduate Award, an award of \$1,000 for the top-performer of this course. He underlines the efficacy of this award, stressing that despite the chaotic return-to-campus situation in that term, this scholarship indeed boosted the students' in-class participation and their interests in tackling cybersecurity-related issues
- Meng Xu has also been invited to several discussions on cybersecurity training hosted by CPI, for both the National Cybersecurity Consortium (NCC) and the Masters in Cybersecurity and Privacy program, and he notes that he looks forward to his future participation in the construction of a WatSPEED cybersecurity certificate program
- For the past three years, Meng Xu has served on the evaluation committee that awards the annual CPI Excellence Graduate Scholarship. He stresses that the strength of applications has been very high each year and that he believes CPI is fulfilling a valuable service by allocating these scholarships to talented students at the institution
- **Xi He**, (MATH/CS) Assistant Professor at the Department of Computer Science, highlights that CPI has made vital initiatives and built resources to drive critical research in cybersecurity and privacy, directly benefiting her research and career.
 - Xi He notes that that CPI has actively engaged Waterloo's expertise in diverse areas, including computer science, engineering, mathematics, cryptography, and quantum computing, with companies through workshops and seminars such as CPI Talks, CPI Spotlights, and CPI RoundTables. Xi He's research group, including her students, has benefited from presenting their research and attending the talks. In particular, they presented their work on APEx for differentially private data exploration in one of the seminars to the industrial partners of CPI, who later shared with them several practical use cases to apply the groups technologies
 - Through CPI's connections with the industry, they have also initialized collaboration with the team at Source Inc on a research proposal, "Scaling Oblivious Query Processing using Differentially Private Indexes," in submission to the Ontario Centre of Innovation. Xi He expects novel prototypes to be developed with their industrial partner and several high-quality publications from this collaboration
 - CPI provides its members and their sponsored students with reliable computing and generous financial support. For example, their research project, CacheDP, a recent submission to a top database conference venue, was fully developed and tested using the Chippie Cluster, a computing cluster provided by CPI. At one of the CPI annual events sponsored by Symcor, Xi He's student received the best poster award for his master thesis on "Differentially Private Learning with Noisy Labels"

4.5 Student Engagement

CPI has a number of initiatives and activities designed to engage with and support students:

- **Scholarships:** further detail in Section 7.2.3.
 - **Graduate Excellence Scholarship** - a scholarship available to graduate students supervised by a CPI researcher who demonstrate excellence in their studies related to cybersecurity and privacy. Past winners include:

- 2022 Bailey Kacsmar
 - 2021 Siddharth Priya & Mahbod Majid
 - 2020 Shannon Veitch
 - 2019 Chang Ge
- **Undergraduate Award Pilot** – a pilot program awarding a scholarship to an undergraduate student who demonstrates excellence in their studies related to cybersecurity and privacy (CS 458 & ECE 458)
- **CPI Talks** – a public outreach lecture series intended for people from all walks of life. CPI Talks are designed to be accessible to anyone, without any background or knowledge in cybersecurity and privacy. They are also intended to provide a way for high school and undergraduate students to better understand and appreciate the interdisciplinary considerations involved in cybersecurity and privacy challenges
- **Communications Channels** – are media channels aimed at engaging with students, consisting of (a) a [cpi-seminars](#) mailing list for announcements and (b) a new [cpi-students](#) mailing list, exclusive to students, which focusses on engaging students with opportunities to network and participate in discussions on cybersecurity and privacy related topics
- **Chippie Cluster** – consists of compute resources used primarily by students who are authorized by CPI members
- **Student Advisory Committee** – is comprised of students from multiple faculties who are engaged in cybersecurity and privacy related research in order to give voice to student concerns and requests for support

Faculty/Unit

Electrical & Computer Engineering

Combinatorics & Optimization

Cryptography, Security, and Privacy (CrySP)

Balsillie School of International Affairs

Department of English Language & Literature, Critical Media Lab

Institute for Quantum Computing (IQC), Physics and Astronomy Department

Faculty of Health; School of Public Health Sciences

Representative

[Behkish Nassirzadeh](#)

[Youcef Mokrani](#)

[Nils Lukas](#)

[Kristen Csenkey](#)

[Alexi Orchard](#)

[Devashish Tupkary](#)

[Pedro Miranda](#)

- **CPI RoundTable Discussions** – are a public lecture series which will also include student-centred events designed to engage and support them

4.6 Community Engagement – General Public

CPI has expanded its engagement with the general public by creating programming that can be digested by anyone, regardless of their familiarity with cybersecurity and privacy issues. These efforts include:

- **Annual Conference** – an annual event CPI organizes every October in conjunction with Cybersecurity Awareness Month. This event generally incorporates themed panel discussions and distinguished speakers from research and industry leaders discussing topics of import in relation to cybersecurity and privacy concerns. It is an opportunity for networking and collaborative inception, as well as student engagement, such as poster sessions where students may present their work publicly. In addition, there are [multiple events](#) throughout the year, in a variety of formats, that include public-facing promotion and encouragement for the general public to engage with cybersecurity and privacy topics
- **CPI Talks** – are a public outreach lecture series. These events create opportunities for people to be informed about and engage with important cybersecurity and privacy issues

- **Public Newsletters** – are produced by CPI on our publicly available website that address cybersecurity and privacy concerns, along with a mailing list [subscription](#)
- **Social Media Presence** – is maintained by CPI through our [Twitter](#), [YouTube](#), and [LinkedIn](#) profiles for online engagement
- **CPI Spotlight Series** – are articles, presented in plain language, that highlight our researchers focussing on their research and ideas in our regular Spotlight Series on our public website
- **CPI-Hosted Events** – are events hosted by CPI on specialized topics of interest to CPI members. The following are examples of CPI-hosted events during the past three years:
 - [Blockchain and Security Workshop](#)
 - [Data and Privacy during a Global Pandemic Conference - Anindya Sen](#) (ARTS/ECON) **Plinio Morita** (HEA/HLTH) **Bessma Momani** (ARTS/PSCI)
 - [Privacy in the era of big data, machine learning, IoT, and 5G](#)
 - [The evolution of cybersecurity in the Covid-19 era - Douglas Stebila](#) (MATH/C&O) **Urs Hengartner** (MATH/CS)
 - [Trustworthy AI security, privacy, and ethics - N. Asokan](#) (MATH/CS) **Maura R. Grossman**, **Xi He** (MATH/CS) **Yaoliang Yu** (MATH/CS) **Vijay Ganesh** (ENG/ECE)
 - [Rising challenges in cybersecurity and privacy practice - Florian Kerschbaum](#) (MATH/CS)
 - [Women in tech - Jennifer Whitson](#) (ARTS/SOC & LS)
 - [Managing the Pandemic through Contact-Tracing Apps: Technological innovation or a Challenge to Privacy and Civil Liberties - Florian Kerschbaum](#) (MATH/CS) **Douglas Stebila** (MATH/C&O) **Plinio Morita** (HEA/HLTH) **Bessma Momani** (ARTS/PSCI)
 - [Privacy, Infrastructures, Policy - Maura Grossman](#) (MATH/CS)
 - [Careers in Cybersecurity and Privacy](#)
 - [UW Workshop True North - Michele Mosca](#) (MATH/C&O)

4.7 Supporting Community Events

CPI regularly supports cybersecurity and privacy events organized by our partner organizations. Examples include the following:

- [ISSTA '21 conference](#) - supported via a CPI Seed Grant – **Heather A. Love** (ARTS/ENGL) **Werner Dietl** (ENG/ECE) **Chengnian Sun** (MATH/CS)
- Cybersecurity and International Affairs Workshops by CPI and the Balsillie School of International Affairs:
 - [Cybersecurity Risk to Physical Infrastructure](#)
 - [Blockchain technology: The Law of Un-intended Consequences](#)
 - [The Surveillance State](#)
 - [Russia, Cyberattacks, and Cryptology: How to better protect our democratic processes?](#)
 - [China, Surveillance, and Censorship Resistance](#)
 - [Borders in Cyberspace](#)
 - [uXperience | Think Privacy](#) - supported via a CPI Seed Grant - **Leah Zhang-Kennedy** (ARTS/STRATFORD SID&B)
- [Investigating Targeted Espionage: Methods, Findings, Implications Panel](#)

5

Member Engagement



In this chapter, we focus on the ways in which CPI engages with and supports its members. CPI prioritizes consistent and open communication within its faculty and student membership with an emphasis on support and feedback. CPI has an [external](#) and an [internal website](#), which facilitates the constant update of both public and membership audiences with pertinent information. We have regular newsletters for [public](#), [member](#), [seminar](#), and [student](#) groups, and we encourage all visitors to our websites to subscribe to the media that they prefer.

CPI has a [YouTube](#), [LinkedIn](#), and a [Twitter](#) account, with dedicated staff that maintain our online social media presence and work in tandem with other UWaterloo entities and cybersecurity and privacy groups to cross-promote related material. CPI also maintains an ongoing [member survey](#) that tabulates feedback on CPI's activities and member opinions as new members join CPI.

5.1 Online Engagement

Our public website serves as our first point of contact for the majority of engagement with CPI. It contains the necessary information for public and member interest and is constantly updated with relevant information on not only CPI and its members activities, but pertinent information in the cybersecurity and privacy sphere.

Our online engagement statistics are as follows:

- **Twitter:** 146 followers
- **YouTube:** 18 subscribers - 770 total views of videos
- **LinkedIn:** 80 followers
- **cpi-members** mailing list: 65 subscribers
- **cpi-students** mailing list: 70 subscribers
- **cpi-seminars** mailing list: 162 subscribers
- **cpi-public** mailing list: 514 subscribers

5.2 Membership Survey

Beginning in Fall of 2021, CPI launched an ongoing [membership survey](#) portal ([Appendix C](#)) that continues to garner responses as CPI adds to its membership base. This survey affords members the opportunity to highlight their respective publications and accomplishments, as well as giving voice to their opinions on what CPI is doing well, and what we can improve upon. Approximately a third of CPI members have responded to this survey, and their opinions were quite consistent in terms of common themes. Members felt that CPI was effectively helping to create opportunities for collaborations and networking, and they were effusive about CPI's Seed Grant program ([Section 7.1.3](#)) and scholarships ([Section 7.2.3](#)), as well as our involvement with the [NCC](#). Additionally, they were enthusiastic about our [CPI Talks](#) and seminars activities and wished to see all of these initiatives strengthened and continued.

In terms of what was posited as areas of potential improvement, the CPI membership believes that there is a perceived need for greater cohesion amongst its members, again focusing on collaborative possibilities, awareness of the work and industry engagements that are at play, and with a pointed human element; members would like to feel that CPI is a community of individuals, with consistent opportunities for social interactions.

Notably, the responses to both questions evidenced a very strong positive trend towards media events and community building. These two concepts should be linked together, as they both involve creating a stronger and more coherent public image that is based on shared interests and collaborative efforts. Opinions were expressed that centered on there being a demonstrable need for CPI to be more publicly visible across multiple venues in aid of multiple benefits, including professional reputation for UWaterloo and CPI, involvement with the NCC, as well as industry and research collaborations. Finally, the issue of access to compute resources and real-world data was at the forefront as a desirable outcome.

5.3 CPI's Response to Feedback

As will be demonstrated in the pertinent sections of this renewal report, CPI has undertaken the necessary steps to address these concerns and will continue to be a proactive and responsive support system for our membership.

- [For Achievements and Directions for Community Building \(Section 6.3.3.1\)](#)
- [For Achievements and Responses to Faculty Feedback \(Section 4.4\)](#)
- [For Achievements and Responses to Student Feedback \(Section 4.5\)](#)
- [For our Seed Grant Program \(Section 7.1.3\)](#)
- [For our Chippie Servers/compute Resources \(Section 7.1.2\)](#)

6

Strategic Directions

In this chapter we delineate CPI's strategic directions, both past and present. CPI's strategic directions have been formulated based on alignment with [UWaterloo's Strategic Priorities](#) and ongoing feedback from CPI members, as well as external feedback from the wide array of interactions thus far. CPI is committed to the ongoing pursuit of excellence and achievement within cybersecurity and privacy research, and our strategic plan reflects our goals of continuing to support and nurture our community in their efforts to enrich knowledge and capabilities within the cybersecurity and privacy sphere. CPI continues to orient its efforts towards addressing the cybersecurity and privacy talent gap and global risks by formulating strategic goals that focus on developing talent and training supports, increasing communications outreach on all fronts, advancing members research efforts through facilitation of grant applications, as well as engaging with interdisciplinary resources and industry partners.

6.1 Status of 2018 Strategic Plan Goals & Objectives

In 2018, CPI initiated its first formal planning process, which resulted in the initial strategic plan. That plan advised the Institute's vision and mission, and detailed specific goals and objectives in the priority areas of research and education. Below, in Table 1 Ch.6 - *Status of 2018 Strategic Plan Goals & Objectives*, we summarize the progress to date with respect to each goal identified in the 2018 strategic plan.

Table 1 Ch.6 - Status of 2018 Strategic Plan Goals & Objectives

GOAL	Progress to Date
To extend UWaterloo's strength and impact in cybersecurity and privacy	<ul style="list-style-type: none"> Facilitated UWaterloo being among top-15 worldwide in research on technological aspects of cybersecurity and privacy Co-led the formation of National Cybersecurity Consortium (NCC) (Section 4.2) Co-led the successful ISED CSIN proposal from NCC
To strengthen existing research collaborations among departments, schools, and faculties, and foster new collaborations, to broaden the research and impact of UWaterloo researchers in all topics related to cybersecurity and privacy	<ul style="list-style-type: none"> Expanded to include 60 researchers from all faculties at UWaterloo Helped to support development of and secure funding for research projects (Section 4.1) with a focus on multidisciplinary initiatives (see cell below) Launched several new community-building initiatives (Sections 4.4 - 4.5) Administered an annual Seed Grant program to bootstrap (especially multidisciplinary) research or training activities (Section 4.4 pg. 21)
To foster external research collaborations with companies, research centres, and others, where appropriate	<ul style="list-style-type: none"> Facilitated the engagement of its members in major sponsorships, investments, and establishment of key partnerships through providing an institutional environment for interdisciplinary research, research team building, connections, and grant development supports. Examples can be found in Section 4.3.1
To facilitate application for institutional-level grants and funding	<ul style="list-style-type: none"> Facilitated major institutional-level proposals such as CFI, ORF-RI, CERC, CFREF, CRC, and other grants, to build on UWaterloo's long-term strength and more recent growth in the research and application of cybersecurity and privacy. Examples can be found in Section 4.3.2
To increase the visibility and strength of UWaterloo's cybersecurity and privacy research to attract the best new faculty and HQP	<ul style="list-style-type: none"> Facilitated the development of talent for a complex future through: <ul style="list-style-type: none"> Existing initiatives like the CPI Excellence Graduate Scholarship (Section 4.5, item i) Launching new CPI Undergraduate Award pilot (Section 4.4 item i) Strengthened sustainable and diverse communities through: <ul style="list-style-type: none"> Existing mechanisms like CPI website, mailing lists, CPI Annual October Conferences, and other targeted events (Section 4.6) Launching new initiatives like CPI Talks, CPI Newsletter, CPI Spotlight Series, CPI RoundTable Discussions, and the CPI Annual October Conference (Section 4.4) CPI has added 20 new members since its inception, with an additional 150+ supervised students (past & present)

6.2 Alignment with UWaterloo's Strategic Priorities

CPI's strategic plan is framed to align with UWaterloo's three strategic themes: **1)** Developing talent for a complex future; **2)** Advancing research for global impact; and **3)** Strengthening sustainable and diverse communities. This strategic plan builds on our foundation in these three intersecting themes for mobilizing change, all with both local and global foci. CPI contributes to each in several ways:

Developing talent for a complex future














- Support CPI members developing new university courses related to cybersecurity and privacy

- Facilitate the development of the UWaterloo Cybersecurity and Privacy MMath degree program
- Collaborate on Upskilling/reskilling programs with [WatSPEED](#)
- Administer [Scholarship](#) and award programs for students

Advancing research for global impact - CPI researchers have contributed to a wide range of cybersecurity and privacy research initiatives

It is important to note that cybersecurity and privacy is inherently interdisciplinary. CPI’s breadth of research expertise reflects that. As such, cybersecurity and privacy concerns permeate through UWaterloo’s strategic priorities, and thusly it may benefit from all different CPI areas of expertise. In Table 2 Ch.6 - *Alignment of CPI Expertise with UWaterloo's Strategic Priorities*, we highlight the examples of the most relevant CPI expertise areas that correspond to each of UWaterloo’s strategic priorities.

Table 2 Ch.6 - Alignment of CPI Expertise with UWaterloo's Strategic Priorities

Strategic Priority	Most Relevant CPI Expertise Areas	
Quantum science, nanotechnology, connectivity, and telecommunications	 Cryptography  Network Security	 Quantum-Safe Communication
Water, energy, and climate: sustainability, security, infrastructure	 Data Science - Security and Privacy  Legal and Policy Aspects of Security and Privacy	 Operational Security
Information technology and its impact, including intelligent systems, human-machine interfaces, cybersecurity, privacy, and data science	All areas of Cybersecurity and Privacy 	
Robotics and advanced manufacturing	 Human & Societal Aspects of Security and Privacy  Software, Hardware, and Systems Security	 Privacy-Enhancing Technologies
Health technologies	 Data Science - Security and Privacy  Operational Security	 Privacy-Enhancing Technologies

Since cybersecurity and privacy are paramount for applied technologies and are inherently interdisciplinary, CPI is continually forming collaborations with internal groups such as: [Robohub](#), [IQC](#), [Waterloo.ai](#), [The Problem Lab](#), and [WatSPEED](#).

CPI will continue in its mission to identify and support interdisciplinary efforts with its members and external partners to achieve research excellence in a multitude of fields.

Strengthening sustainable and diverse communities - CPI continues to develop support systems and community building for its members, as well as supporting students involved with cybersecurity and privacy research.

6.3 Strategic Directions (2022 to 2027)

CPI is currently renewing its strategic plan. A bottom-up, participatory process has been designed to ensure faculty members have the opportunity to reflect on past achievements and challenges and to identify strategic directions and priorities for the future.

6.3.1 Summary of Faculty Survey

Beginning on Dec. 1, 2021, CPI members were encouraged to complete a [survey](#) (summary in [Appendix C](#)), that queried their thoughts on what CPI was doing well and what we could improve upon; we also incorporated various expressions of opinion from informal member sources that were identified as useful. Three dominant themes emerged in their responses. Primarily, CPI members are both positively inclined towards and most interested in Seed Grants (Section 7.1.3) and [Scholarships](#) (Section 7.2.3), followed closely by CPI events, such as our Speaker Series and CPI talks, and finally with a trend towards industry/collaborations and engagement with the NCC. Given the CPI member perceptions with regard to the importance of Seed Grants, as well as scholarships, CPI has expanded the scope of both our Seed Grant and scholarships programs.

CPI has significantly broadened its efforts in events and community building, launching initiatives like [CPI Talks](#), [CPI Spotlight Series](#), and [CPI RoundTable Discussions](#), as well as increasing its online and social media presence. CPI is also planning a recurring slate of events, including public-facing and CPI member/student engagements. The [NCC](#) was repeatedly mentioned as an entity of interest, evidencing that CPI members are invested in the significance of the NCC and its activities. Finally, the issue of access to the Chippie cluster and real-world data was emphasized as desirable. CPI has responded to these concerns, and along with the previously mentioned increase of social and networking opportunities for members, students, and the public, CPI is actively working with the NCC to achieve its goals, and we are adding more compute resources to our current hardware cluster.

6.3.2 Strategic Directions & Initiatives 2022 to 2027

Table 3 Ch.6 - *Strategic Directions & Initiatives 2022 to 2027* illustrates the seven primary goals of CPI's Strategic Directions Plan for 2022-2027. It is rank-ordered and contains general concepts that are linked to more detailed examples in Section 6.3.3, following this table. The second column contains a list of current/example initiatives corresponding to each goal. The list is not intended to be exhaustive and is subject to adaptation and revision during the strategy period in response to changing circumstances and evolving priorities.

Table 3 Ch.6 - Strategic Directions & Initiatives 2022 to 2027

Goals	Example Initiatives
Strengthen Engagement with CPI Community (Section 6.3.3.1)	General: <ul style="list-style-type: none"> • CPI collaborative physical space to increase community and engagement • Effective communication channels, including Team team(s), and mailing lists for KM/KT & community building • EDI-R focus on increasing representation and inputs • Regular CPI RoundTable Discussions to facilitate small-group discussions among CPI members, possibly with other centers/institutes/groups on topics of common interest Faculty: <ul style="list-style-type: none"> • Monthly Executive Director e-mails to update members • CPI Spotlight Series with highlights on CPI members • Faculty Advisory committee to advise CPI leadership • Early Career Researcher support Students: <ul style="list-style-type: none"> • Scholarships & awards • Student Advisory committee to provide feedback on matters of interest to students • Student events, such as poster sessions (for presenting research results), hackathons (for skill development), and mentoring
Nurture NCC (Section 6.3.3.2)	<ul style="list-style-type: none"> • Help operationalize NCC and offer advice and guidance once it is operational
Facilitate Excellence in Cybersecurity and Privacy Research (Section 6.3.3.3)	<ul style="list-style-type: none"> • Chippie cluster expansion • Continued Seed Grant (Section 7.1.3) program • Facilitating applications for institutional-level grants
Facilitate Strengthening/Broadening Cybersecurity and Privacy Training (Section 6.3.3.4)	<ul style="list-style-type: none"> • Support for the development of new university courses and degree programs on cybersecurity and privacy • Upskilling/reskilling with WatSPEED • Scholarships/awards
Build Partnerships (Section 6.3.3.5)	<ul style="list-style-type: none"> • Industry engagement – promote/facilitate industry engagement with CPI researchers • Partnerships with other UWaterloo institutes/centers, and with selected international cybersecurity/privacy centers • EDI-R – promoting external partnerships to create funding for EDI-R initiatives, such as targeted scholarships
Influence Public Policy (Section 6.3.3.6)	<ul style="list-style-type: none"> • Engagements with Centre for International Governance Innovation, governmental bodies, UWaterloo partners, Institute of Public Administration of Canada • Outreach and media – creating awareness and influencing policy makers/public opinion • Workshops, blogs, press releases, public dissemination - supporting engagement that promotes policy change

Promote Cybersecurity and Privacy Awareness (Section 6.3.3.7)	<ul style="list-style-type: none"> • Public and internal websites • Social media presence – Twitter, YouTube, LinkedIn • Public newsletters and mailing list • CPI Talks - Public outreach lecture series • CPI RoundTable Discussions • Hosting Annual Conference, and supporting community events • CPI Spotlight Series featuring CPI researchers
--	---

6.3.3 Strategic Directions & Initiatives 2022 to 2027 – Expanded Detail

In this section, we provide more detail on each of the goals identified in Table 3 Ch.6 - *Strategic Directions & Initiatives 2022 to 2027*.

6.3.3.1 Strengthen Engagement with CPI Community

As a result of surveys and interviews with CPI members (described in Section 5), there will be a stronger focus on all aspects of community building within CPI’s strategic directions. Our membership supports the expansion of not only academic, research, and industry engagements and collaborative efforts, but an increased focus on social and networking opportunities across a broad spectrum.

General Engagement

A clear theme that emerged from our discussions with CPI members is their wish that CPI would help foster a sense of community among its members and their students, extending beyond facilitating research and academic initiatives. CPI is committed to expanding its networking and engagement schedule to improve community access both internally and externally, as well as providing community-strengthening events.

Ongoing

- Creating opportunities for industry to sponsor CPI activities such as conferences or innovation competitions/hack-a-thons

Under Consideration

- Obtain a collaborative physical space – for events, and informal gatherings, available for CPI members and their students
- Facilitating seminars for UWaterloo students – on topics from the different CPI expertise areas
- Creating mentorship activities with graduate & undergraduate students
- Identifying and addressing EDI-R concerns:
 - Implementing voluntary anonymous surveys to identify gaps/barriers/demographics
 - Creating opportunities for support as guided: such as outreach/community spaces
 - Pursuing community assigned scholarships and resources/outreach
 - Pursuing increased visibility/participation/volunteers in Campus events: job fairs etc.
- Continuing [CPI Spotlight Series](#) to regularly highlight ongoing innovations of our members
- Continuing CPI Talks & CPI RoundTable Discussions – events to encourage dialogue and networking among CPI researchers and with external entities. CPI Talks are public events, CPI RoundTable Discussions are invitation-based events and may include students for specific instances

Faculty Engagement

CPI continues to provide and develop member-specific support initiatives geared towards addressing their needs, including community building and networking assistance.

Ongoing

- Maintaining [Faculty advisory committee](#) to solicit advice regarding CPI operations and strategy (est. 2021)

- Supporting Early Career Researchers as detailed in (Section 4.4)

Under Consideration

- Promoting CPI members recreational events: once a term mixer, board game night, video game tournament

Student Engagement

CPI embraces its role in supporting UWaterloo students in their pursuits of educational advancement in cybersecurity and privacy. Based on student feedback, CPI will continue to expand on its community building developments and educational supports.

Ongoing

- Administering [Graduate excellence scholarships/targeted scholarships](#) (Section 7.2.3) for underrepresented communities
- Administering [Graduate student advisory committee](#) to advise CPI leadership on matters concerning students

Under Consideration

- Working with [Graduate student advisory committee](#) members to explore education or outreach initiatives with local schools

Equity, Diversity, Inclusivity, & Anti-Racism Initiatives

CPI understands that the issues surrounding cybersecurity and privacy are not limited to technological innovation and development, there is a significant human component that is integral to every interaction with technology. CPI is committed to supporting researchers and research in an equitable and inclusive manner.

Ongoing

- Creating EDI-R policy (Section 9) with consultation from UWaterloo advisors
- Maintaining relationships with underserved community leaders and establishing goals with their guidance
- Pursuing ethical and appropriate engagement with all stakeholders, communities, and entities
- Promoting open-door policy on input – CPI will clearly and continually state that we encourage anyone to reach out to us with ideas and concerns
- Maintaining ongoing engagement with communities, stressing that they are partners and gatekeepers in our approaches to initiatives that involve them

Under Consideration

- Creating anonymous voluntary surveys on gaps/barriers/demographics for CPI membership and students
- Creating opportunities for support as guided: such as outreach/community spaces
- Pursuing Community assigned scholarships and resources/outreach
- Promoting research that explores the impacts of technology on marginalized communities, through a cybersecurity and privacy lens

6.3.3.2 Nurture NCC

CPI's involvement has been integral to the formation of the [NCC](#) and its success in being named the lead recipient of ISED's [CSIN](#) program. CPI will maintain its leadership role in NCC as it evolves. See (Section 4.2) for further details on NCC.

Ongoing

Intensive start-up phase (2022) – this includes:

- Supporting the NCC organization's hiring, marketing, legal, and program development
- Start-up activities for CPI members' 13 proposed shovel ready projects
- Leveraging a business development manager (Section 11.3.1) focusing on the unique opportunities the NCC will offer in training, commercialization, and research

Planned

- Providing advice to NCC's leadership team and Board of Directors; serve on various advisory committees of NCC (2023 and later), leverage CPI's strategic fund of Seed Grants (Section 7.1.3), and training content (Section 7.2) through NCC funding programs

6.3.3.3 *Facilitate Excellence in Cybersecurity & Privacy Research*

CPI is committed to expanding the networking, collaborative, and research opportunities for its membership, including supports for grant applications and KM/KT dissemination. CPI central staff consulted with members to determine the best configurations and supports that can be of most use to CPI members.

Ongoing

- Financed and set up significant compute resources ([Chippie cluster](#)) for use by CPI researchers and their students (Section 7.1.2)
- Financing and implementing the Seed Grant program (Section 7.1.3)
- Facilitating applications for institutional-level grants, including networking and project support from CPI staff (Section 4.3)
- Facilitating interdisciplinary collaboration including networking and project support from CPI staff: e.g., [Robohub – CPI RoundTable Discussion](#): topics on security and privacy in robotics
- Exploring feasibility of providing research support services (Section 7.1.1)

Under Consideration

- Expanding the [Chippie cluster](#) (Section 7.1.2) based on CPI member needs
- Sponsoring student research paper competitions on cybersecurity and privacy issues of societal interest
- Planning outreach activities with ISED Canada and the Office of the Privacy Commissioner of Canada to understand their priorities and help encourage research on policy issues of high priority
- Extending interdisciplinary collaboration: e.g., with Waterloo.ai, Problem Lab, and other similar units

6.3.3.4 *Facilitate Strengthening/Broadening Cybersecurity and Privacy Training*

CPI is actively developing and promoting the upskilling of industry professionals, as well as expanding the educational opportunities for UWaterloo students at the Graduate & Undergraduate levels.

Ongoing

- Administering the [CPI Excellence Graduate Scholarships](#) program (Section 7.2.3)
- Administering a pilot for a CPI Undergraduate Award during 2022 (Section 7.2.3)
- Co-ordinating the UWaterloo training proposal with NCC
- Implementing [CPI RoundTable Discussion](#) with this focus
- Planning the 2022 CPI Annual Conference with cybersecurity/privacy talent gap as a primary theme – Future CPI Annual Conferences with different themes

Under Consideration

- Defining potential CPI professional training offerings by aligning faculty interests and capacities with identified needs in collaboration with WatSPEED (Section 7.2.2)
 - Facilitating collaboration of CPI members with WatSPEED
- Developing a stronger role in cybersecurity training
 - Supporting emerging cybersecurity/privacy courses and programs like the new cybersecurity and privacy MMath program

6.3.3.5 *Build Partnerships*

As part of its ongoing mandate to support CPI researchers and cybersecurity and privacy innovations, CPI is focused on creating and maintaining positive supportive relationships with a broad spectrum of partners. Currently, CPI has minimal direct sponsorship, due in no small part to an enhanced focus on the NCC followed by a total change of staff since its inception. However, the current CPI staffing roster has addressed these concerns, with the Executive Director, Managing Director, and recently hired Associate Director positions highlighting that a focused effort in this area is necessary, and is a core component of CPI's ongoing goals and its renewal plan.

Develop Strategic International Partnerships Under Consideration

- Targeting academic partnerships in US, Europe, Asia, and Africa with a view to encouraging grassroots level collaboration and enhance competitiveness of joint calls for proposals from international funding opportunities
- Exploring and developing partnerships: e.g., CERIAS at Purdue University

Refine Interaction with Industry Partners Ongoing

- Revamping CPI's industry partnership model. The draft new model has three levels of sponsorships:
 - Scholastic Sponsors will fund a Graduate Excellence Scholarship or a set of undergraduate awards (Section 7.2.3)
 - Corporate Sponsors will connect more closely with CPI members in a chosen expertise area while also funding events, awards, and scholarships
 - CPI Partners will be deeply connected to the CPI membership and community through options for a named chair, consulting, and student engagement
- Creating a policy to streamline the process for managing industry requests
- Continuing pursuit of interdisciplinary collaboration and expanding the offering of services, for example:
 - IQC – CPI collaborations with industry and internally
 - Continuing [CPI RoundTable Discussions](#)

6.3.3.6 *Influence Public Policy*

CPI is committed to actively engaging with policymakers at all echelons of influence in supporting their decision-making efforts in relation to matters of cybersecurity and privacy. CPI's Associate Director will utilize and demonstrate thought leadership principles based on his expansive experience and comprehensive government and industry connections whilst leading this new initiative. See [Appendix D](#) for further details.

Planned

- Working with CIGI to organize a pan-Canadian conference on cybersecurity and privacy with the federal and provincial governments to help CPI members understand how their expertise can contribute to governmental policymaking
- Organizing meetings with relevant UWaterloo units (such as Waterloo.ai and IQC) to discuss ways to coordinate efforts on policy-related research
- Organizing workshops which will take all the policy relevant research done by CPI researchers and then map them to common sub themes to encourage research partnerships and applications for funding
- Creating a blog series consisting of a specific policy theme to communicate the big picture of research findings with societal implications
- Investigating the possibility of constructing more 2-minute videos to further disseminate research findings (2 videos currently available – [here](#) and [here](#))

- Meeting with organizations such as the Institute of Public Administration Canada to understand public policy needs regarding cybersecurity and privacy research

6.3.3.7 *Promote Cybersecurity and Privacy Awareness*

A foundational aspect of CPI's strategic plan is grounded in promoting not only the efforts of CPI's membership, but to consistently expand the public awareness of the issues surrounding cybersecurity and privacy. CPI will continue to develop its role as a platform that promotes the thought leadership activities of its members, focusing on constantly supporting and disseminating the results of their development of expertise, experience, and credibility in the sphere of cybersecurity and privacy.

Ongoing

- Facilitating the presentation of research results at conferences for CPI members
- Creating and offering presentations from CPI staff that expand on and promote CPI initiatives
- Continuing with regular offerings of [CPI Talks](#)
- Promoting availability of CPI members for media interviews
- Maintaining and improving CPI's web and social media presence across multiple platforms such as [Twitter](#), [YouTube](#), and [LinkedIn](#)
- Highlighting the work of CPI's researchers through press releases and pursue external media prospects
- Focusing on strengthening CPI community with newsletters and researcher updates
- Continuing our [CPI Spotlight Series](#)

Under Consideration

- Increasing profile with external stakeholders and the media by regularly providing perspectives or opinion on related matters – Pursuing opportunities to participate in discussions in public media
- Increasing recognition and profile by acknowledging the achievements of faculty and students, and facilitating opportunities for faculty and students to be affiliated with CPI (e.g., publications, presentations) – [CPI Spotlight Series](#) articles
- Increasing engagement with the local community by developing and implementing a community outreach program, including consideration of a public event series – Promoting [CPI Talks](#) in local media
- Offering short term (1-2 days to 1-2 weeks) programs in the summer for all levels of students
- Creating opportunities for grad/undergrad/high school/elementary volunteers
- Creating and promoting digital presentation packages to be sent to schools/media outlets - with or without a presenting CPI rep
- Pursuing sponsorship/direct involvement with external events such as:
 - Waterloo-Wellington Science & Engineering Fair
 - Canada-Wide Science Fair

7

Activities and Services

In this chapter we expand on the activities and services of CPI. In cybersecurity and privacy, UWaterloo distinguishes itself in two respects:

- UWaterloo is a Canadian leader and has achieved worldwide reputation as a leading centre for research in cybersecurity and privacy technologies (csrankings.org)
- UWaterloo has unparalleled multidisciplinary breadth in cybersecurity and privacy, allowing it to both understand and confront core cybersecurity and privacy challenges in different application areas including engineering, healthcare, financial, and other sectors, and to be able to do so through an interdisciplinary approach covering technological, social, economic, and policy aspects

CPI's role is to build on these strengths by:

- serving as a comprehensive facilitator for external and internal inquiries, collaborations, and sponsorships about cybersecurity and privacy, which creates more opportunities for its members
- building a sense of community among its members which increases the opportunities for them to undertake research and training wherein each individual complements the others
- helping its members to undertake or participate in large initiatives with many moving parts, made possible through the central management and bridging of CPI. For example, the NCC (see [Appendix B](#)), was successful through internal collaborations that were only possible through CPI's active leadership

To fulfill this role effectively, CPI offers multiple activities and services in research, education, and communications as described below.

7.1 Research

CPI continues to support its members in their research efforts through the following initiatives:

- Recognizing, facilitating, and supporting researchers with collaborative opportunities including through our [CPI RoundTable Discussions Series](#) (Section [4.3.1](#))
- Providing a fertile environment for the training of multi-faceted HQP
- Creating and maintaining links to funding sources (Section [4.3.2](#))
- Identifying partners and soliciting letters of support for research projects
- Aiding in the construction of effective research proposals
- Providing leadership and management for research projects and promoting interdisciplinary initiatives
- Providing support highlight options to faculty, such as communications, knowledge mobilization, and knowledge translation
- Offering centralized assistance to CPI member research projects and collaborative efforts
- Offering short-term technical research support, cross-faculty student to member communication and connection, and student event coordination through a Research Support Specialist
- Identifying, creating, and supporting partnerships/sponsorships in the public and private sectors (Section [4.3](#))
- Providing space and support for academic delegations and academic visitors
- Offering CPI as a central hub of contact for cybersecurity and privacy related inquiries

7.1.1 Research Support Services

In Fall 2021, CPI started an initiative to explore the demand and feasibility for clear and direct specialized technical support to help CPI researchers on technical and student engagement matters. A graduate student was recruited part-time during the September 2021-December 2022 period to conduct this exploration. Through a combination of one-on-one and group interviews, as well as [survey results](#), CPI identified the research support functions of greatest interest, which were for services in or adjacent to:

- Open-source project development and management
- Software development for research
- Assistance with obtaining data
- Hosting social functions and community building for students including:
 - Introductions to target users or communities
 - “Capture the Flags” and hackathons

Despite several members expressing great interest in such support, including for particular projects, when attempting to engage with pilot projects, the response from members became far more muted. The problem appears to be that whilst many researchers want such support available, few wish to experiment with it, and would rather have a well-established resource to draw from. Therefore, CPI will not continue with the research support services role. CPI will continue dialogue with its members and consider this role in the future.

7.1.2 Chippie Cluster – Compute Resources

Compute resources are hardware infrastructure resources that provide processing capabilities in the cloud. For example, virtual clusters, virtual resource pools, and physical servers are all compute resources. As part of CPI’s commitment to supporting our researchers and affiliated graduate students, CPI has purchased several powerful processors (CPUs) with graphics processing units (GPUs). This is known as the “Chippie cluster”.

- Chippie cluster GPUs are utilized for their extremely high computational processing abilities and are employed by researchers who require this processing power to run simulations and manage complex data operations
- The Chippie cluster is managed by the Computer Science Computing Facility (CSCF) and includes access scheduling and maintenance duties
- Current GPUs we have available in the Chippie cluster:
 - 8x NVIDIA RTX A6000: Purchased July 2021 \$6800 each
 - 6x NVIDIA A100: Purchased March 2021 \$12500 each

Our member survey outlined a strong desire from the majority of the respondents to increase Chippie cluster compute resources, leading to CPI expanding them.

- CPI is expecting delivery of two more A100 processors in the near future
- Current usage of all Chippie cluster resources is approx. 50% and is increasing, with spikes of usage often hitting 100% at times
- Additionally, expansion of the Chippie cluster will see the addition of a CPU-centric system with 224 CPU cores and 6TB of RAM. With this system addition, we can evaluate usage of CPU-heavy computation resources and scale GPU/CPU resources appropriately

7.1.3 Seed Grant Program

The mission of CPI is to facilitate collaborative research in cybersecurity and privacy amongst researchers across the entire University and with companies, leading research centres, government agencies, and other institutions in Canada and internationally.

Starting in 2022, CPI is using the seed grants program to incentivize collaborative research across academic units by encouraging proposals that incorporate this multidisciplinary approach.

CPI regularly calls upon its members to submit such proposals for small Seed Grants that can be used to facilitate:

- Early-stage proposal preparation
- Networking
- Discussions
- Training

The CPI Seed Grant program has been running since 2019 and has funded 12 projects with a total disbursement of \$226,893

Table 4 Ch.7 - *CPI Seed Grant Recipients* details the Seed Grants that have been disbursed to date.

Table 4 Ch.7 - CPI Seed Grant Recipients

Year	Project Title	Primary Investigator(s)	Status
2018	Cybersecurity, Privacy, and International Affairs	Bessma Momani & Michele Mosca	Completed
	Knowledge Mapping and Data Visualization	Jennifer R. Whitson	Dissolved
	Security and Privacy in Public-targeted Information Tracking (SANDPIT)	Ian Goldberg & Jennifer R. Whitson	Completed
2019	Bridging Policy and Technical Gaps: Information Asymmetry or Head in the Sand?	Bessma Momani & Michele Mosca	Completed
	Waterloo Workshops at the Intersection of Security, Blockchain, and Machine Learning	Vijay Ganesh	Completed
2020	Conference - What Governments Can do to Protect Individual Privacy and Encourage Data Innovation	Anindya Sen	Ongoing
	Data and Privacy During a Global Pandemic Conference	Anindya Sen	Completed
	UXperience Think Privacy	Leah Zhang-Kennedy	Completed
2021	Collaborative, Secure Software Development	Leah Zhang-Kennedy	Ongoing
	Cybersecurity, Privacy, and Countering Disinformation	Bessma Momani & Michele Mosca	Ongoing
	Pathways for Black Youth to Careers in Cybersecurity and Computer Science	Maura R. Grossman	Ongoing
2022	An Interdisciplinary Approach to Developing the Privacy and Security of Mobile Health Apps: A Pilot Investigation	Adam Molnar & Yousra Aafer	Ongoing
	Workshop on Interdisciplinary Approaches to Cybersecurity and Privacy	Adam Molnar & Urs Hengartner	Ongoing

2018 Cybersecurity, Privacy, and International Affairs - This project created a research cluster, whose objective was to create a platform to enable experts in the fields of technology (computer scientists and mathematicians), and international affairs (scholars on geopolitics, security, and defence threats), to work together to establish policy strategies to contain or deter cyberattacks. This research group is now in a Partnership Grant led by Université de Montréal named The Human-Centric Cybersecurity Partnership (HC2P)

Knowledge Mapping and Data Visualization - The first stage of this project was a fact-finding mission for the Institute, identifying the research areas and interconnections of the existing CPI community. The second stage was to identify core themes and values, bringing them to a core set

of CPI members for initial feedback, and then shaping them into a draft mission statement. The third stage would have been drafting a mission statement and soliciting wider CPI feedback, as well as drafting metrics for measuring CPI progress. The PIs, in consultation with CPI leadership, decided to dissolve the project when one of the PIs left UWaterloo.

Security and Privacy in Public-targeted Information Tracking (SANDPIT) - Media, government, and industry commonly frame Security and Privacy as diametrically opposed: protecting one requires sacrificing the other. This misconception persists despite cybersecurity and privacy to the contrary, as well as an emphasis on data as the ‘new oil’ propelling both technological and economic development, further sidelining privacy concerns. This conference brought together CPI researchers, local industry, government, and NGOs, as well as Canadian academics working in the field to **1)** emphasize privacy as fundamental in cybersecurity practice, **2)** highlight how government and industry data-collection can generate “toxic assets” rather than profitable resources, and **3)** align privacy and cybersecurity goals in terms of research collaborations that involve partnerships with industry and government. This project also yielded the [Privacy, Infrastructures, Policy](#) event in Feb 2020.

2019 Bridging Policy and Technical Gaps: Information Asymmetry or Head in the Sand? - This project undertook a comprehensive review of the current state of academic and policy literature on why society needs to understand the risks, opportunities, and related ethical questions raised by the adoption of emergent and disruptive technologies, such as quantum computing. It focused on what ways might emerging technologies affect the behaviour of citizens in all aspects of their lives, institutions, and governments; and focussed on how can citizens, organizations and governments balance the competing needs of security and privacy in an increasingly ‘open’ and democratic society. The following related funding applications were successful:

- Cybersecurity and Privacy Institute’s workshop funding - Event on Cybersecurity, Privacy, and Countering Disinformation
- Department of National Defence Targeted Engagement Grant - Cybersecurity Threat to Canada’s Critical Infrastructure

Waterloo Workshops at the Intersection of Security, Blockchain, and Machine Learning -

This grant covers the facilitation of two separate workshops:

“Waterloo Workshop on Security & Blockchain” (Oct 5-6, 2019) This workshop had two themes: security of blockchain technologies (e.g., methods to automatically find security defects in smart contracts) and the use of blockchain as a substrate for security primitives (e.g., PKI). There were also talks on the development of completely new blockchains, where security and privacy concerns are addressed in their design from the ground up. The speakers were world-leaders in these topics from the following institutions: Waterloo, Toronto, ETH Zurich, National University of Singapore, IBM, as well as many leading blockchain start-up companies.

“Waterloo ML & Security & Verification Workshop” (Aug 26-30, 2019) This workshop also had two themes: the first is the use of ML in verification, program analysis, and security analysis methods. The second theme is the use of verification and analysis techniques to discover vulnerabilities and construct adversarial inputs against ML models. The speakers were world-leading researchers from: Waterloo, Toronto, MIT, Stanford, CMU, Georgia Tech, UPenn, National University of Singapore, Wisconsin, MUN, Kiel, Perimeter Institute, and Google Brain.

2020 Conference - What Governments Can do to Protect Individual Privacy and Encourage Data Innovation - Research funding will be used to organize a virtual conference of experts from different disciplines to present research findings and recommendations on policies that can encourage data-based innovation by Canadian firms, as well as federal and provincial governments, while protecting individual privacy. This conference will bring together experts from the social sciences, humanities, computer science, statistics, and legal sector who will provide feedback to

governments on recent privacy legislation, as well as help frame policy recommendations on future initiatives. Specifically, there will be a focus on the recently introduced **Digital Charter Implementation Act**, which proposes a number of new policies that impact businesses and consumers.

Data and Privacy During a Global Pandemic Conference - This virtual conference was organized by the Master of Public Service Policy & Data Lab and GEDI and was sponsored by the Waterloo Cybersecurity & Privacy Institute. It brought together experts from the social and physical sciences, computer science and engineering, statistics, and law to help frame policy recommendations for a variety of societal issues that have emerged with COVID-19, such as what needs to be done in order to curb the spread of Covid-19, par ex., exposure notification, legal considerations, and statistical modeling.

UXperience Think Privacy - Think Privacy was a design jam that engaged high school and post-secondary students to explore, collaborate, and propose solutions to address the central question: “How might we create transparency, trust, and meaningful consent in the connected world?” Participants worked in small interdisciplinary teams spanning across diverse backgrounds. Workshops, presentations, and mentorship provided participants with opportunities to learn about privacy-preserving approaches to existing and emergent technology. There is a cybersecurity talent shortage, due to inadequate promotions and education in high schools as well as universities about cybersecurity as a career path. Furthermore, women are severely underrepresented in the field. Hackathons and design jams provide highly focused bursts of public engagement. These events demonstrate educational opportunities to encourage millennials and industry participation in cybersecurity and privacy challenges.

2021 Collaborative, Secure Software Development - Software security is influenced by various actors beyond the software developer. This project proposes investigating how interdisciplinary teams (e.g., developers, designers, engineers, security analysts) work collaboratively to design, develop, test, and maintain secure software. The project's objectives are to understand how practitioners collaborate on security-related tasks, explore methodologies and processes used that influence software security and identify opportunities and barriers for effective secure software development in team-based environments. Originally one year; grant extension granted 2021-2023.

Cybersecurity, Privacy, and Countering Disinformation - States and their proxies are increasingly engaging in disinformation and undermining public trust in Canadian institutions and our democracy. Cybersecurity, privacy, and disinformation are of great concern, but there has been a dearth of dedicated conversations at the intersection of these domains. This workshop will discuss the crucial questions arising from the interplay between personal cybersecurity, growing use of disinformation, and the need to preserve privacy in the name of protecting civil liberties. The added need for this workshop is that technological solutions to private messaging apps are less effective than those applied to public social media. There are [known regulatory solutions](#) to stem disinformation, but their efficacy has been debated and is often ineffective on private messaging apps. There is also concern about attempts to control quantum-safe cryptography (a defense) or quantum computing (a potential offense) in disinformation campaigns.

Pathways for Black Youth to Careers in Cybersecurity and Computer Science - The proposed program will teach Black youth in Ontario about cybersecurity and highlight different career pathways available to them in that area, as well as in computer science more generally. This grant will be used to make material adjustments to the content and delivery of an existing program and to offer the program again in early 2023 to a larger cohort (at least 30 students). The goal is to provide opportunities for Black youth in Ontario who would not otherwise be exposed to potential

careers in cybersecurity and computer science, who would like to develop a stronger understanding of what a career in these fields might entail and to help them better position themselves for academic and career opportunities. A longer-term goal is to improve Waterloo's School of Computer Science's diversity admissions statistics. This project also aims to develop and offer at least three internship opportunities with a participating company or multiple companies from our industry partners for students who are successful in the program and would like to expand on their learning.

2022 An Interdisciplinary Approach to Developing the Privacy and Security of Mobile Health Apps: A Pilot Investigation The shift toward digital healthcare delivery, amplified by the COVID-19 pandemic, adds an unprecedented urgency to understanding the cybersecurity and privacy implications of digital healthcare technologies. Mobile health apps in particular facilitate healthcare services through a hybrid range of private and public providers, increasingly delivered in private spheres such as the home, and through private personal devices such as mobile phones and tablets. These trends complicate privacy and introduce security risks for business, governments, clinicians, and patients alike. Through an innovative interdisciplinary combination of researchers from Computer Science, Sociology, and Law, and an industry partner Otekha Health Corporation, this project provides a pilot investigation into how the technical design, operation, and use of mHealth apps intersect with existing regulations to facilitate secure and private use of mHealth apps in Canada.

Workshop on Interdisciplinary Approaches to Cybersecurity and Privacy This project will receive funding (to be supplemented by a SSHRC Connections Grant) to organize a three-day workshop at the University of Waterloo, entitled "Developing Interdisciplinary Approaches to Cybersecurity and Privacy Research and Regulation". This workshop will invite leading researchers, practitioners, and graduate students from across computer science, the social sciences, and law/policy to discuss their experiences working in interdisciplinary team settings on issues of cybersecurity and privacy. Participants will share strategies, successes, and challenges of incorporating interdisciplinary approaches into their work and will generate new approaches to collaboration that can meaningfully inform scholarly research, professional training, and the development of integrated regulatory initiatives.

CPI particularly encourages interdisciplinary work spanning technological, social, economic, political, and human aspects of cybersecurity and privacy that lead to tangible impacts, as well as improving UWaterloo's reputation as a leader in cybersecurity and privacy.

7.2 Training

As part of CPI's commitment to addressing the cybersecurity and privacy talent gap, CPI is actively supporting numerous initiatives that engage UWaterloo students as well as professionals in the private sector.

7.2.1 University Courses

In reference to addressing the talent gap in cybersecurity and privacy, CPI is supporting the development of several new university courses and the Cybersecurity and Privacy MMath degree program. These activities are part of the UWaterloo training proposal (coordinated by CPI) that has been submitted to the NCC's call for training programs.

7.2.2 Professional Upskilling and Reskilling

University training is complemented by workforce training. CPI has identified this as a priority with the following future initiatives, with CPI's Associate Director leading the following activities:

- CPI is participating in a new nationwide upskilling/reskilling grant proposal with WatSPEED: ISI Upskilling for Industry (UII) Program
 - WatSPEED and CPI would use our expertise and capacity to support the scaling-up and delivery of upskilling activities across regions and sectors
 - This program will fund one or more proposals for 3 years and up to \$250M
- Planning to provide professional upskilling and reskilling by leveraging material from the Cybersecurity and Privacy MMath degree program currently in development by CPI members including material on the following topics:
 - Networking & Cloud fundamentals
 - Cryptography
 - Network security and cloud-based networking
 - Systems security and architecture (anti-virus encryption)
 - Methodology for writing secure code
 - Privacy regulations, effects on stakeholders, and risk management
- In June 2022, CPI organized a [RoundTable Discussion](#) on these topics bringing CPI researchers and WatSPEED together for in-depth discussions. Outcomes included:
 - Planning to offer training content for the Certified Information Systems Security Professional certification
 - Planning to offer upskilling content for C-Suite level clients based on next generation cybersecurity threats and technologies

7.2.3 Scholarships & Awards

CPI Excellence Graduate Scholarships

The mission of CPI is to facilitate excellence in collaborative research in cybersecurity and privacy. In order to support our graduate students and reward their excellence, CPI has been running the [Cybersecurity and Privacy Excellence Graduate Scholarship](#) since 2019.

- This scholarship is open to graduate students of CPI members and supports each recipient with \$10,000 CAD for one academic year
- To date, 5 scholarships worth a total of \$50,000 have been awarded
- Scholarships are typically funded by gifts from industry partners. Past donors towards the CPI Excellence Scholarships program include BlackBerry, Symcor, and CPI

Cybersecurity and Privacy Institute Undergraduate Award Pilot

CPI is exploring the feasibility of setting up an Undergraduate Award Program to recognize top performers in undergraduate cybersecurity and privacy programs. The awards, valued at \$1000 each, are intended to encourage students to take and excel in cybersecurity and privacy courses, and for them to engage with CPI.

- A pilot project to examine the feasibility of establishing and expanding the program is currently under way
 - During Winter 2022, CS 458 (a large undergraduate course in computer science) participated in the pilot
 - During Spring 2022, the pilot has been expanded to include ECE 458 (another large undergraduate course)

The results thus far are promising. On successful conclusion of the pilot, CPI will initiate discussions with potential donors to set up a sustainable award program starting in 2023.

7.3 Communications

In support of CPI's stated goals of increasing cybersecurity and privacy awareness and engagement, as well as promoting the efforts of CPI researchers and supported initiatives, CPI is committed to the following efforts as a thought leader in the cybersecurity and privacy space, with a focus on maintaining its leadership role and engaging with current research directions.

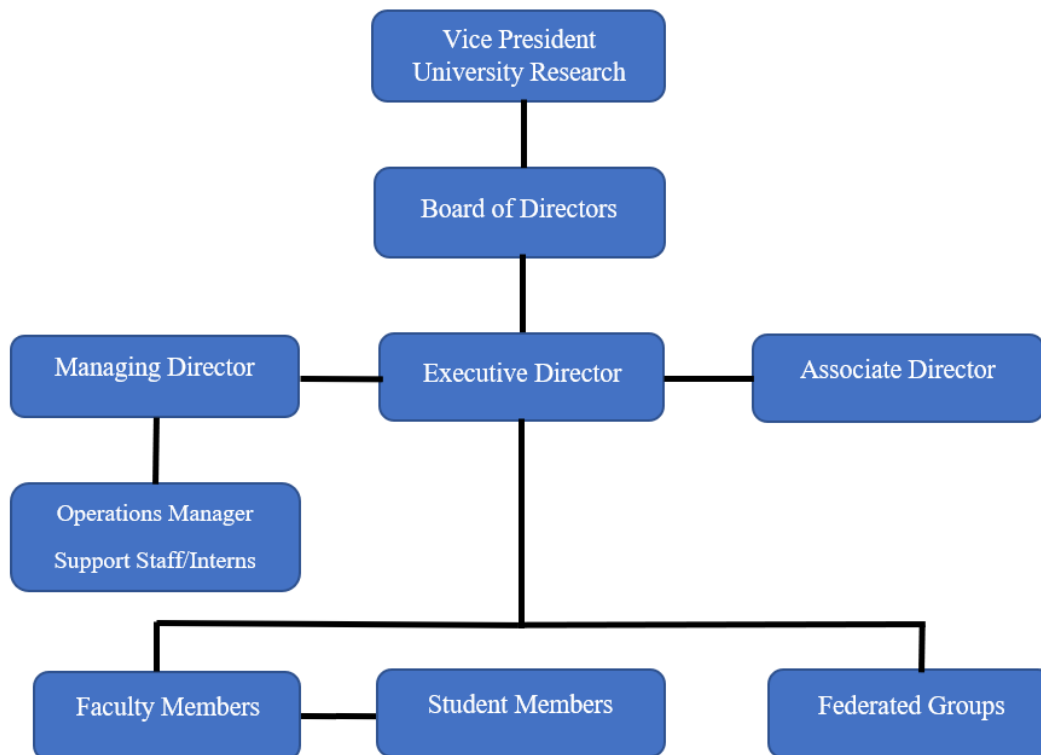
- Providing a comprehensive media strategy that promotes CPI, researcher, and student initiatives through our online presence creating events, social media, newsletters etc.
- Promoting members and their activities through our [CPI Spotlight Series](#) and other UWaterloo channels, such as the [Daily Bulletin](#)
- Building on the public facing image and reputation of CPI and UWaterloo as leaders in cybersecurity and privacy research
- Supporting and organizing [CPI Talks](#), public outreach lecture series, conferences, and events, including lecture exchanges with other entities in the cybersecurity and privacy sphere
- Strengthening and enabling undergraduate and graduate student activities, as well as community building efforts
- Increasing the visibility and strength of UWaterloo's cybersecurity and privacy research to attract the highest quality new faculty and HQP
- Engaging government policymakers and industry in discussions about the importance of addressing cybersecurity and privacy threats, and the opportunity to incorporate and export solutions

8

Governance

In this chapter we explain the governance and structure of CPI. The governance structure of CPI was initially established in the Cybersecurity and Privacy Institute (CPI) proposal (2018) in conformance with the University's Policy 44 on Research Centres and Institutes.

8.1 Structure



The organizational structure of the Cybersecurity and Privacy Institute is comprised of:

Members: faculty members drawn from all Faculties, whose research is primarily focused on cybersecurity or privacy, or whose research impacts, applies, or studies the impact of cybersecurity and privacy. Student members are included in the cpi-students mailing list, which is open to all UWaterloo students with an interest in cybersecurity and privacy.

Federated Groups: UWaterloo research labs, groups, centres, or institutes primarily focused on cybersecurity or privacy. Normally all members of such groups would be eligible to be members of CPI, based on their research.

*Note: Two federated groups, the Centre for Applied Cryptographic Research (CACR) and the Cryptography, Security, and Privacy Research Group (CrySP), were the federated groups identified at the inception of CPI. However, as of 2022, CACR has been dissolved.

Executive Director: a cybersecurity and privacy researcher of international stature, who is also a faculty member.

Associate Director: a researcher selected from CPI membership who holds regular faculty appointments at the University of Waterloo at a faculty other than the faculty of the ED at the time of the AD’s appointment., reporting to the Executive Director.

Management and Administrative Staff: a Managing Director, reporting to the Executive Director, for institute activities and collaborations, as well as for managing CPI staff, and a communications coordinator/administrative assistant, reporting to the Managing Director. Support staff and/or interns (reporting to the Managing Director) may be hired to help with operations. Research staff may be hired as needed, to support initiatives with industry and other partners.

8.2 Reporting Structure & Board Composition

In accordance with Policy 44, the Executive Director will report to the CPI Board of Directors which will be chaired by the Vice President, Research and International, or their designate.

The CPI Board of Directors includes:

- Vice President, Research and International (Chair)
- Dean of Mathematics (ex-officio)
- Dean of Engineering (ex-officio)
- Dean of Arts (ex-officio)
- One other Dean, chosen from the Deans of Science, Environment and AHS (ex-officio)
- Executive Director of CPI
- A representative of CrySP Research Group
- 3 Members-at-Large

The director position for one of the Dean of Science, Dean of Environment and Dean of AHS will rotate every two years, with selection made by the Chair of the Board.

The three Members-at-Large will be nominated by a subcommittee of the Board and elected by a majority of the Board members. One will be replaced each year, so the duration at steady state is three years. One principle to be followed in the nominations is to help ensure representation from a breadth of research interests across the Institute. Another principle is to meet the diversity and gender targets of the University in selecting the representatives.

8.3 Current Board Members

Category	Member
Vice President University Research (Chair)	Charmaine Dean
Dean of Mathematics (ex-officio)	Mark Giesbrecht
Dean of Engineering (ex-officio)	Mary Wells
Dean of Arts (ex-officio)	Sheila Ager
Dean Faculty of Environment	Bruce Frayne
Executive Director of CPI	N. Asokan
A representative of CrySP Research Group	Ian Goldberg
Member-at-Large	Adam Molnar (Term expiring 2023)
Member-at-Large	Ian McKillop (Term expiring 2022)
Member-at-Large	Michele Mosca (Term expiring 2022)

9

EDI-R Mission Statement

Within this chapter we discuss the ongoing work in Equity, Diversity, Inclusivity & Anti-Racism that CPI has undertaken.

CPI's EDI-R Mission Statement

CPI understands that the issues surrounding cybersecurity and privacy are not limited to technological innovation and development, there is a significant human component that is integral to every interaction with technology. CPI believes that technology exists for the sole purpose of improving the lives of everyone equally and equitably, and we understand that there are dramatic inequalities that exist in this world that manifest in myriad ways within the different spheres of technology. Whether it be an inequitable level of technological access due to socioeconomic status or geographical location for example, or the vastly differing degrees of access to educational opportunities, CPI understands that any initiative we are a part of must be mindful of these inequalities, and the part we play in addressing them. CPI is committed to supporting researchers and research in an equitable and inclusive manner and we welcome the opportunity to engage with individuals and organizations from all walks of life and support them in their efforts to increase their knowledge and develop their ideas.

Our efforts in achieving our EDI-R goals include:

Ongoing

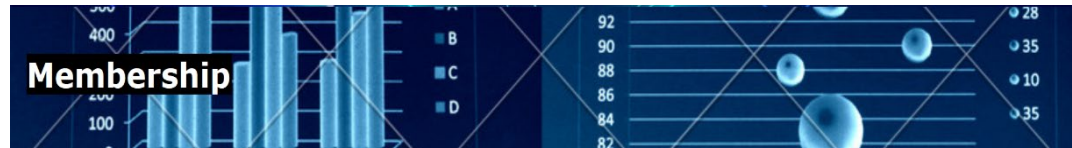
- Drafting EDI-R policy with consultation from UWaterloo advisors (Tamara Zur, Emily Burnell, Sarah Grzincic, Sara Anderson, Veronica Kitchen, Bessma Momani, Jermal Jones)
- Establishing relationships with underserved community leaders and established goals with their guidance
- Creating ethical and appropriate engagement with all stakeholders, communities, and entities
- Maintaining and promoting open-door policy on input – CPI will clearly and continually state that we encourage anyone to reach out to us with ideas and concerns
- Establishing ongoing engagement with communities, stressing that they are partners & gatekeepers in our approaches to initiatives that involve them
- CPI Staff have engaged with significant EDI-R related UWaterloo programming including:
 - Introduction to Equity
 - Disrupting and Decentering Whiteness
 - Unlearning the Binary: Fostering a Truly Trans-Inclusive Campus
 - 2SLGBTQ+ Fundamentals Workshop
 - Pathways for Addressing (with care) Disclosures of Racism – Faculty & Staff Workshop
 - You Don't Know What You Don't Know
 - Pathways for Addressing with care disclosures of racism

Under Consideration

- Creating anonymous surveys on gaps/barriers/demographics - CPI membership and students
- Creating opportunities for support as guided: outreach/community spaces
- Creating community assigned scholarships and resources/outreach
- Promoting research that explores the impacts of technology on marginalized communities, through a cybersecurity & privacy lens

Please see [Appendix A](#) for an examination of the breadth of our membership in terms of academic diversity.

10



Within this chapter we outline the CPI's membership particulars.

10.1 Membership Categories

Membership in CPI is open to faculty members interested in cybersecurity and privacy in any academic unit at the University of Waterloo, including two types of membership.

Members: who identify themselves as active researchers in some aspect of cybersecurity or privacy, and students interested/involved with cybersecurity and privacy issues.

Affiliates: who are working in adjacent areas but are interested in cybersecurity or privacy.

CPI members and affiliates benefit from the interdisciplinary relationships, awareness, and collaboration made possible by the existence and activities of the Institute. CPI serves as a facilitator for external inquiries, collaborations, and sponsorships in relation to CPI topics of interest, which creates more opportunities for CPI's membership. The cohesive approach and multidisciplinary breadth made possible by CPI will enable its members to undertake research wherein each individual complements the others. CPI organizes regular events for the benefit of its members, affiliates, and the broader community, such as events to mark Cybersecurity Awareness Month, and the [CPI Talks](#) public outreach lecture series.

Faculty members whose research is related to cybersecurity and privacy, by advancing the science and technology, by applying cybersecurity and privacy, or by studying the impact of security and privacy on society, policy, or the economy, are eligible for membership.

For example, sociologists studying the behavior of hackers or insiders who provide access to intruders are welcome as members. Policy experts who are curious about the formation of national policy relating to anonymity of customers, ownership of social media content or regulation about the adoption of quantum-safe cryptosystems are also welcome. Actuarial scientists studying risk in cyberassurance would be eligible for membership, as would software engineers building more robust software with an eye to reducing vulnerabilities and intrusion.

All students and researchers affiliated with CPI members or affiliates are automatically eligible to benefit from CPI resources and services relevant to them such as joining the [cpi-students mailing list](#), applying for [CPI Excellence Graduate Scholarships](#), and enrolling to make use of the [Chippie cluster](#).

Benefits and Responsibilities of Membership

Members and affiliates will benefit from the interdisciplinary relationships, awareness and collaboration made possible by the existence and activities of the Institute, and will enjoy the following benefits:

- participation in the annual Seed Grant (Section 7.1.3) competition intended to bootstrap multidisciplinary research and training in cybersecurity and privacy
- their graduate students may apply for [CPI Graduate Excellence Scholarships](#)
- may sponsor students and researchers in their groups to make use of the [Chippie cluster](#)
- invitations to meet with external stakeholders (people from industry, government, media, or other organizations)

The Leadership team (Executive Director, Associate Director, and Managing Director), the administrative staff, and others, will form a comprehensive single point of contact for external inquiries, collaborations and sponsorships, about cryptography, security, and privacy, which will create more opportunities for members.

Members will be responsible to advance UWaterloo's overall agenda in cybersecurity and privacy, by participating as enthusiastic members of the Institute. This includes participating in Institute activities to communicate research results, interact with research sponsors, and become aware of receptor organizations' security and privacy needs. Members are expected to act as ambassadors by communicating the breadth and excellence of the work of Institute members in a constructive way.

10.2 Faculty Members

Name	Status	Affiliation	Expertise Areas
Yousra Aafer	Member	MATH/CS	Software, hardware, and systems security; Mobile and IoT Security
Mark Aargaard	Member	ENG/ECE	Security, Cryptography
Gordon Agnew	Member	ENG/ECE	Cryptography; Data science security and privacy; Network security; Privacy-enhancing technologies; Quantum-safe communication; Block chains
Ehsan Amjadian	Affiliate	MATH/CS	Data science security and privacy; Privacy-enhancing technologies; Software, hardware, and systems security,
N. Asokan	Member	MATH/CS	Software, hardware, and systems security; Privacy-enhancing technologies; Data science security and privacy
Diogo Barradas	Member	MATH/CS	Network security; Privacy-enhancing technologies
Efrim Boritz	Member	ARTS/ACCT	Operational Security
Raouf Boutaba	Member	MATH/CS	Network security; Software, hardware, and systems security
Phil Boyle	Affiliate	ARTS/SOC & LS	Legal and policy aspects of security and privacy; Human and societal aspects of security and privacy
Sarah Burch	Affiliate	ENV/GEOG & ENVM	Legal and policy aspects of security and privacy; Human and societal aspects of security and privacy
Alec Cram	Member	ARTS/ACCT	Human and societal aspects of security and privacy; Operational security
Werner Dietl	Member	ENG/ECE	Software, hardware, and systems security
Sebastian Fischmeister	Member	ENG/ECE	Security
Vijay Ganesh	Member	ENG/ECE	Data science security and privacy; Human and societal aspects of security and privacy; Legal and policy aspects of security and privacy; Software, hardware, and systems security
Catherine Gebotys	Member	ENG/ECE	Software, hardware, and systems security
Ian Goldberg	Member	MATH/CS	Cryptography; Privacy-enhancing technologies

Guang Gong	Member	ENG/ECE	Cryptography; Network security; Privacy-enhancing technologies; Software, hardware, and systems security; Quantum-safe communication; Lightweight cryptography, pseudorandom generation
Sergey Gorbunov	Member	MATH/CS	Cryptography; Network security
Maura R. Grossman	Affiliate	MATH/CS	Human and societal aspects of security and privacy; Legal and policy aspects of security and privacy
Arie Gurfinkel	Member	ENG/ECE	Software, hardware, and systems security; Formal Methods and Static Analysis
Mohammad Hajiabadi	Member	MATH/CS	Cryptography; Quantum-safe communication
Anwar Hasan	Member	ENG/ECE	Software, hardware, and systems security; Quantum-safe communication; Cryptography
Xi He	Member	MATH/CS	Data science security and privacy; Privacy-enhancing technologies; Cryptography
Urs Hengartner	Member	MATH/CS	Data science security and privacy; Human and societal aspects of security and privacy; Network security; Privacy-enhancing technologies
David Jao	Member	MATH/C&O	Cryptography; Quantum-safe communication
Thomas Jennewein	Member	SCI/PHYS & ASTRO	Quantum Safe-Communication
Gautam Kamath	Member	MATH/CS	Data science security and privacy; Privacy-enhancing technologies
Koray Karabina	Affiliate	MATH/C&O	Cryptography; Data science security and privacy; Privacy-enhancing technologies; Quantum-safe communication
Florian Kerschbaum	Member	MATH/CS	Data science security and privacy
Veronica Kitchen	Affiliate	ARTS/PSCI	Human and societal aspects of security and privacy; Legal and policy aspects of security and privacy
Nasser Lashgarian Azad	Affiliate	ENG/SYDE	Software, hardware, and systems security;
Debbie Leung	Affiliate	MATH/C&O	Cryptography; Quantum-safe communication; Quantum cryptography
Heather A Love	Member	ARTS/ENGL	Human and societal aspects of security and privacy; Pedagogy of responsible innovation, Interdisciplinary collaboration between STEM and humanities
Norbert Lutkenhaus	Member	SCI/PHYS & ASTRO	Quantum Safe-Communication
Ali Mashtizadeh	Member	MATH/CS	Software, hardware, and systems security; Operating Systems, Distributed Systems
John McLevey	Member	ENV/KI	Data science security and privacy; Human and societal aspects of security and privacy
Ian McKillop	Member	HEALTH	Operational security

David McKinnon	Affiliate	MATH/PM	Cryptography
Alfred Menezes	Member	MATH/C&O	Cryptography; Quantum-safe communication
Adam Molnar	Member	ARTS/SOC & LS	Human and societal aspects of security and privacy; Legal and policy aspects of security and privacy
Bessma Momani	Member	ARTS/PSCI	Human and societal aspects of security and privacy; Legal and policy aspects of security and privacy
Plinio Morita	Member	HEA/HLTH	Human and societal aspects of security and privacy; Legal and policy aspects of security and privacy; Privacy-enhancing technologies
Michele Mosca	Member	MATH/C&O	Cryptography; Quantum-safe communication
Mei Naggapan	Member	MATH/CS	Software, hardware, and systems security
Marcel O'Gorman	Affiliate	ARTS/ENGL	Human and societal aspects of security and privacy; Privacy-enhancing technologies
Anindya Sen	Member	ARTS/ECON	Data science security and privacy; Human and societal aspects of security and privacy
Sherman Shen	Member	ENG/ECE	Network security; Privacy-enhancing technologies
Douglas Stebila	Member	MATH/C&O	Cryptography; Network security; Quantum-safe communication
Doug Stinson	Member	MATH/CS	Cryptography
Theo Stratopoulos	Member	ARTS/ACCT	Human and societal aspects of security and privacy; Data science security and privacy; Privacy-enhancing technologies
Chengnian Sun	Member	MATH/CS	Software, hardware, and systems security
Mahesh Tripunitara	Member	ENG/ECE	Security
Stacey Watson	Member	MATH/CS	Human and societal aspects of security and privacy; Network security;
Jennifer R. Whitson	Member	ARTS/SOC & LS	Human and societal aspects of security and privacy
Bernard Wong	Member	MATH/CS	Network security; Software, hardware, and systems security
Meng Xu	Member	MATH/CS	Operational security; Software, hardware, and systems security
Jon Yard	Affiliate	MATH/C&O	Cryptography; Quantum Safe-Communication
Yaoliang Yu	Member	MATH/CS	Data science security and privacy; Privacy-enhancing technologies
Hongyang Zhang	Member	MATH/CS	Data science security and privacy; AI security
Leah Zhang-Kennedy	Member	ARTS/STRAT FORD SID&B	Human and societal aspects of security and privacy

11



Within this chapter we report CPI’s past financial details from 2017/18 - 2021/22 and establish CPI’s future financial plans for 2022/23 - 2026/27. CPI operates on a limited budget, its major expenses being administrative salary and initiatives that support researchers, and research development. CPI also awards seed grants and scholarships every year.

11.1 CPI’s Initial Budget (2018)

CPI currently receives no industry money for operational purposes. CPI’s sponsors have contributed to awards, scholarships, and other activities managed by CPI listed in the program expenses. Currently, CPI has a carry-forward totalling \$520,858. This carry-over is due to a number of unexpected staffing turnover factors that coincided with the pandemic, and a delayed infrastructure purchase for our Chippie cluster (Section 7.1.2), now slated for the 2022/23 fiscal year. CPI anticipates that the carry-forward will be fully expended in the next five years with projected increases in programming, services, office, and salary expenses, as well as other initiatives.

Table 5 Ch.11 - *CPI’s Financial Details from 2017/18 - 2021/22* below provides financial particulars related to the activities of CPI for its initial five years.

Table 5 Ch.11 - CPI’s Financial Details from 2017/18 - 2021/22

Income Sources	FY 2017-18	FY 2018-19	FY 2019-20	FY 2020-21	FY 2021-22
Funding					
Provost Support	\$ 258,900	\$ 350,000	\$ 350,000	\$ 343,000	\$ 350,000
Carryforward		\$ 242,397	\$ 371,027	\$ 336,698	\$ 451,193
Sponsorship		\$ 75,000	\$ 20,000	\$ 20,000	\$ 10,000
Other Support		\$ 10,000	\$ 44,800		
Total Funds In	\$ 258,900	\$ 677,397	\$ 785,827	\$ 699,698	\$ 811,193
Expenses					
Salary Expenses	\$ 10,679	\$ 135,298	\$ 278,028	\$ 96,765	\$ 149,907
Office Expenses	\$ 159	\$ 23,828	\$ 10,264	\$ 98,564	\$ 71,132
Program Expenses	\$ 5,665	\$ 147,244	\$ 160,837	\$ 53,176	\$ 69,296
Total Expenses	\$ 16,503	\$ 306,370	\$ 449,129	\$ 248,505	\$ 290,335
Year End Uncommitted Funds	\$ 242,397	\$ 371,027	\$ 336,698	\$ 451,193	\$ 520,858

11.2 Proposed 5-year Budget Plan for CPI

Over the next five years, CPI anticipates significant growth in our faculty membership and student engagement, as well as an increase in research supports and resulting impacts. These goals, coupled with our stated commitment to addressing the global risks in cybersecurity and privacy issues, as well as the cybersecurity and privacy talent gap, are factored into our anticipated budgetary needs. As CPI continues to support initiatives that affect policy change and public awareness of cybersecurity and privacy issues, we foresee our expenses pivoting to reflect these goals. Our five-year financial projection is detailed below with consistent base funding over the next five years, as the subsequent Table 6 Ch. 11 - *CPI’s Financial Plan from 2022/23 - 2026/27* outlines.

Table 6 Ch. 11 - CPI's Financial Plan from 2022/23 - 2026/27

Category	FY 2022-23	FY 2023-24	FY 2024-25	FY 2025-26	FY 2026-27
Funding					
Provost Support	\$ 350,000	\$ 350,000	\$ 350,000	\$ 350,000	\$ 350,000
Carryforward	\$ 520,858	\$ 332,589	\$ 189,222	\$ 24,941	\$ 10,497
Sponsorship	\$ 25,000	\$ 40,000	\$ 40,000	\$ 65,000	\$ 90,000
Total Funds In	\$ 895,858	\$ 722,589	\$ 579,222	\$ 439,941	\$ 450,497
Expenses					
Salary Expenses	\$ 248,704	\$ 409,367	\$ 386,281	\$ 327,444	\$ 336,368
Office Expenses	\$ 236,065	\$ 24,000	\$ 71,000	\$ 17,000	\$ 17,000
Program Expenses	\$ 78,500	\$ 97,000	\$ 97,000	\$ 85,000	\$ 95,000
Total Expenses	\$ 529,367	\$ 533,367	\$ 554,281	\$ 429,444	\$ 448,368
Year End Uncommitted Funds	\$ 332,589	\$ 189,222	\$ 24,941	\$ 10,497	\$ 2,129

11.3 Budget Explanation

11.3.1 Salary Expenses

Staff salaries encompass the expenses for the following CPI positions. Since its inception, CPI has grown steadily in terms of staffing needs, as evidenced by the addition of a new managing director in 2021 and an associate director in 2022. The repeated hiring of interns/students to fulfill the roles of GRA, support staff, and research support specialist, attest to the increasing responsibilities CPI is undertaking. However, the research support role (Section 7.1.1), will be discontinued by end of December 2022.

Current Positions:

Executive Director
Associate Director
Managing Director
Operations Manager

Casual Staff/Co-op Student (GRA/Research Support Specialist)

CPI envisions that with the responsibilities and demands that the NCC will continue to create, the following two positions will become necessary.

Business Development Manager – CPI is at the onset of a critical time-window to jump-start industry partnerships that can support (a) helping CPI members partner with industry players to develop compelling research and commercialization proposals for funding opportunities, especially from NCC, which is expected to start funding projects by 2023, (b) substantially expanding the sponsorship for CPI's undergraduate/graduate scholarships and student awards (Section 7.2.3), and events (Section 7.3). To this end, CPI has identified a need for a short-term (two years) business development manager who will focus on creating and supporting relationships with other entities in the cybersecurity and privacy sphere to create a strong group of industry partners for our members who are eager to partner with industry. This will include training, sponsorship, consulting, and research opportunities, for example. This is envisaged as a fixed-term position intended to help bring CPI to a steady-state of industry engagement.

Communications Manager – During 2022, CPI employed a part-time communications specialist who helped to substantially improve CPI's communication mechanisms. To retain this momentum, CPI has identified the need for a full-time communications manager who will be responsible for an increased focus

on public facing engagement and media responsibilities, including revamping the website, internal and external newsletters, effective and persistent social media presence, member spotlights, and support of policy (Section 7.3). To this end, CPI has proposed a short-term (one year) communications manager to start in November 2022. The expectation is that as sponsorship in CPI increases, the funding generated will meet the threshold of supporting the position becoming permanent.

11.3.2 Office Expenses

Funds allocated to the following areas include a varied array of expenditures that are directly related to CPI operations and services, including the Chippie cluster, telephone, supplies, printing, advertising, and promotional efforts, along with office equipment acquisitions. Additionally, CPI has budgeted for the following:

Professional Development/Training – CPI encourages its staff to grow professionally and promotes opportunities for its staff that also align with CPI’s goals.

Note: FY 2024-25 - \$40K allocated to a collaboration space (Section 6.3.3.1). This is in tandem with the CFREF/A grant that is supporting the Molnar initiative outlined in Section 4.1.3.

11.3.3 Program Expenses

Funds allocated to the following areas in program expenses refer to costs primarily related to administering specific CPI research and support activities, as well as a range of events, including [CPI RoundTable Discussions](#) and our [Annual October Conferences](#).

Other expenses include:

Seed Grant Program – Funds for administering CPI’s Seed Grants program (Section 7.1.3). With the NCC funding projected to end in 2025, CPI has allocated an increase in funding to the Seed Grants program in FY 2024-25 through to 2026-27 to bootstrap new research initiatives.

CPI Student Scholarships – Funds allocated for student scholarships as required (Section 7.2.3).

Honoraria – CPI offers honoraria to speakers and other persons who contribute to CPI’s initiatives.

Travel – On occasion, staff members of CPI are called upon to travel to external events.

Events – CPI offers regular in-person programming and events that require catering and support services.

11.3.4 Steady State Budget Beyond 2027

The steady state budget beyond 2027 (Table 7 Ch.11 - *Steady State Budget from 2027*) reveals that CPI has planned for long-term operational consistency for our membership base at UWaterloo. Our goal is to maintain similar office expenses and adapt our program expenses to the current budget model. However, factoring in yearly salary increases for CPI staff while provost support remains the same, CPI’s budget will be difficult to maintain without additional external funding. Therefore, we see industry sponsorship as one option to support CPI’s growth.

We have been conservative in our estimates of industry sponsorship over the next 5 years and beyond 2027 so that we can plan our operations with consistency. The sponsorship funding is planned to grow from \$40,000 to \$130,000 based on a FY 2022/23 ramp up and future projections. Furthermore, with increased sponsorship funding, we anticipate an opportunity to grow our Scholarship, Seed Grant, and other offerings (allocated in Program Expenses), and to employ a full-time permanent communications manager (allocated in Salary Expenses).

For clarity, (Table 7 Ch.11 - *Steady State Budget from 2027*) contains a steady state budget model from 2027 forward.

Table 7 Ch.11 - Steady State Budget from 2027

Confirmed Funds & Commitments	Steady State Beyond 2027
Funds In	
Provost Support	\$ 350,000
Carryforward	
Sponsorship	\$ 130,000
Total Funds In	\$ 480,000
Funds Out	
Salary Expenses	\$ 343,000
Office Expenses	\$ 22,000
Program Expenses	\$ 115,000
Total Funds Out	\$ 480,000
Year End Uncommitted Funds	\$ -

12

Conclusions

The strength of cybersecurity and privacy at UWaterloo is two-fold:

- the outstanding level of research accomplishments in cybersecurity and privacy technologies, which sets UWaterloo significantly ahead of other post-secondary institutions in Canada and among the top ones in the world (evident from csrankings.org)
- the breadth of disciplinary expertise covered by CPI members who approach cybersecurity and privacy concerns through many different lenses (par ex., policy, legal, or usability perspectives) or for many different sectors and application domains (par ex., health, finance, automotive, or national security)

CPI endeavours to provide a forum wherein these twin strengths can be leveraged to benefit CPI members and the university as a whole. CPI contributes directly to the continued recruitment of experts at all levels who possess specific cross-disciplinary expertise in cybersecurity and privacy research, which will stand the University of Waterloo in an even stronger position to be able to address the myriad and difficult slate of cybersecurity and privacy challenges ahead, such as the ones envisioned in UWaterloo's recent CFREF initiative focusing on health.

CPI brings cybersecurity and privacy experts from different disciplines together so that they may engage in dialogues and effectively collaborate to solve difficult problems. CPI's record so far since its inception in 2018, as laid out in this document, underscores the importance of CPI's role in achieving these goals. Therefore, we request that CPI be extended for a further five-year term, allowing CPI to sharpen its effectiveness in facilitating UWaterloo's excellence in cybersecurity and privacy.

13

Appendices

Appendix A Membership Visuals

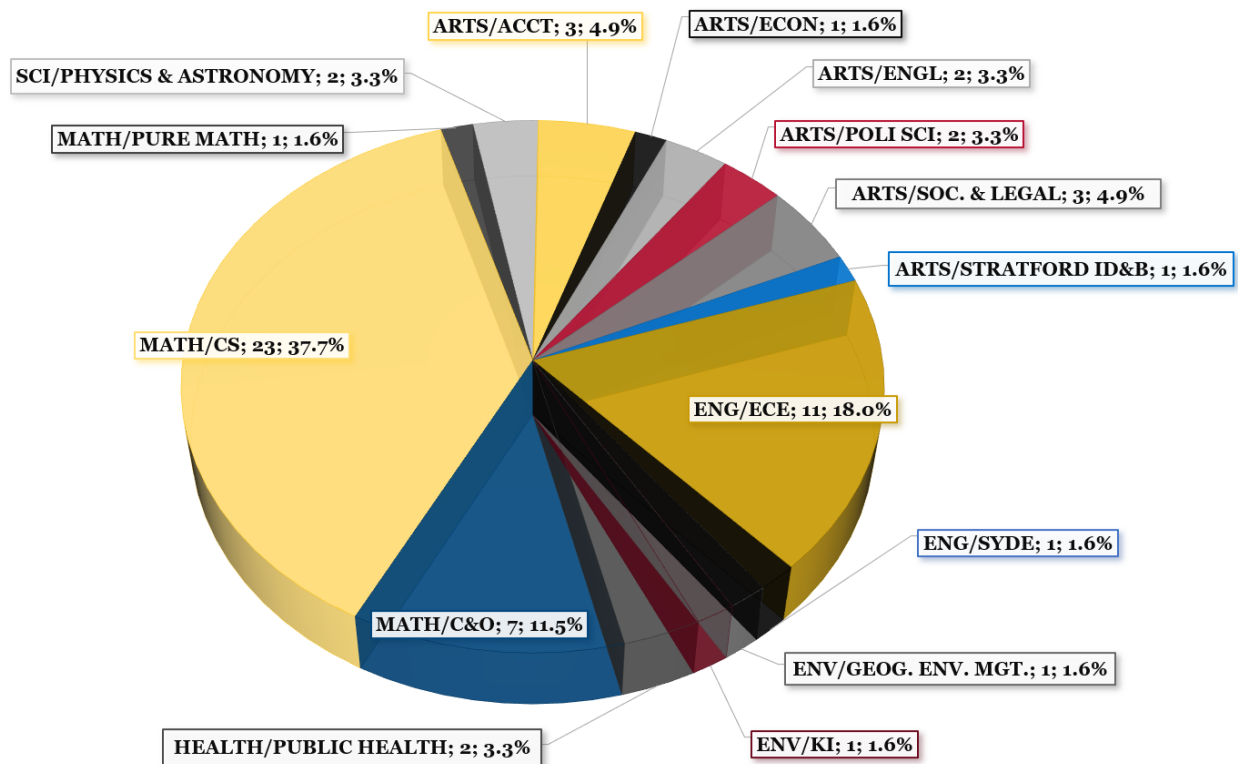
Membership by Department		
Arts	Accounting	3
	Economics	1
	English	2
	Political Science	2
	Sociology & Legal Studies	3
	Stratford School of Interaction Design & Business	1
Engineering	Electrical & Computer Engineering	11
	Systems Design Engineering	1
Environment	Geography & Environmental Management	1
	Knowledge Integration	1
Health	Public Health	2
Math	Combinatorics and Optimization	7
	Computer Science	23
	Pure Math	1
Science	Physics & Astronomy	2

DEPARTMENT	Researcher	Email
ARTS/ACCT	Efrim Boritz	jeboritz@uwaterloo.ca
	Alec Cram	wacram@uwaterloo.ca
	Theo Stratopoulos	tstratop@uwaterloo.ca
ARTS/ECON	Anindya Sen	asen@uwaterloo.ca
ARTS/ENGL	Heather Love	heather.love@uwaterloo.ca
	Marcel O'Gorman	marcel@uwaterloo.ca
ARTS/POLI SCI	Veronica Kitchen	vkitchen@uwaterloo.ca
	Bessma Momani	bmomani@uwaterloo.ca
ARTS/SOCIOLOGY & LEGAL STUDIES	Phil Boyle	philip.boyle@uwaterloo.ca
	Adam Molnar	adam.molnar@uwaterloo.ca
	Jennifer Whitson	jwhitson@uwaterloo.ca

ARTS/STRATFORD SCHOOL OF INTERACTION DESIGN & BUSINESS	Leah Zhang-Kennedy	lzhangkennedy@uwaterloo.ca
ENG/ECE	Mark Aagaard	maagaard@uwaterloo.ca
	Gordon Agnew	gbagnew@uwaterloo.ca
	Werner Dietl	werner.dietl@uwaterloo.ca
	Sebastien Fischmeister	sebastian.fischmeister@uwaterloo.ca
	Vijay Ganesh	vganesh@uwaterloo.ca
	Catherine Gebotys	cgebotys@uwaterloo.ca
	Guang Gong	ggong@uwaterloo.ca
	Arie Gurfinkel	arie.gurfinkel@uwaterloo.ca
	Anwar Hasan	ahasan@uwaterloo.ca
	Sherman Shen	sshenn@uwaterloo.ca
	Mahesh Tripunitara	tripunit@uwaterloo.ca
ENG/SYDE	Nasser Lashgarian Azad	nlashgar@uwaterloo.ca
ENV/GEOGRAPHY & ENVIRONMENTAL MANAGEMENT	Sarah Burch	sarah.burch@uwaterloo.ca
ENV/KI	John McLevey	john.mclevey@uwaterloo.ca
HEALTH/PUBLIC HEALTH	Plinio Morita	plinio.morita@uwaterloo.ca
	Ian McKillop	ian@uwaterloo.ca
MATH/C&O	David Jao	djao@uwaterloo.ca
	Koray Karabina	koray.karabina@uwaterloo.ca
	Debbie Leung	wcleung@uwaterloo.ca
	Alfred Menezes	ajmenez@uwaterloo.ca
	Michele Mosca	michele.mosca@uwaterloo.ca
	Douglas Stebila	dstebila@uwaterloo.ca
	Jon Yard	jyard@uwaterloo.ca
MATH/CS	Yousra Aafer	yousra.aafer@uwaterloo.ca
	Ehsan Amjadian	ehsan.amjadian@uwaterloo.ca
	N. Asokan	nasokan@uwaterloo.ca
	Diogo Barradas	diogo.barradas@uwaterloo.ca
	Raouf Boutaba	rboutaba@uwaterloo.ca
	Ian Goldberg	iang@uwaterloo.ca
	Sergey Gorbunov	sergey.gorbunov@uwaterloo.ca
	Maura R. Grossman	maura.grossman@uwaterloo.ca
	Mohammad Hajiabadi	mdhajiabadi@uwaterloo.ca
	Xi He	xi.he@uwaterloo.ca

	Urs Hengartner	urs.hengartner@uwaterloo.ca
	Gautam Kamath	gckamath@uwaterloo.ca
	Florian Kerschbaum	florian.kerschbaum@uwaterloo.ca
	Ali Mashtizadeh	Mashti@uwaterloo.ca
	Mei Nagappan	mei.nagappan@uwaterloo.ca
	Doug Stinson	dstinson@uwaterloo.ca
	Chengnian Sun	cnsun@uwaterloo.ca
	Frank Tompa	fwtompa@uwaterloo.ca
	Stacey Watson	stacey.watson@uwaterloo.ca
	Bernard Wong	bernard@uwaterloo.ca
	Yaoliang Yu	yaoliang.yu@uwaterloo.ca
	Meng Xu	meng.xu.cs@uwaterloo.ca
	Hongyang Zhang	hongyang.zhang@uwaterloo.ca
MATH/PURE MATH	David McKinnon	dmckinnon@uwaterloo.ca
SCI/PHYSICS & ASTRONOMY	Thomas Jennewein	tjennewe@uwaterloo.ca
	Norbert Lutkenhaus	nlutkenhaus@uwaterloo.ca

Membership by Department



Appendix B National Cybersecurity Consortium

In February of 2022, Innovation, Science and Economic, Development Canada (ISED) announced that the National Cybersecurity Consortium (NCC) was awarded \$80 million over four years through their Cyber Security Innovation Network Program (CSIN). Through the leadership of CPI and four other founding cybersecurity institutes and centres across Canada, the NCC was formed to bridge all cybersecurity expertise across Canada. The CSIN program will ensure Canada is globally competitive and establishes its leadership role in cybersecurity, allowing for the cyber-resilience of our critical infrastructure, privacy and safety of citizens' data, and the safety and assurance of our digital ecosystems.

History and Mandate

In 2020, under the leadership of the previous executive director, Florian Kerschbaum, CPI began to collaborate with four other major Canadian university-based cybersecurity centres and institutes to begin the formation of a national network of cybersecurity networks. This network would be led by:

- Cybersecurity and Privacy Institute, University of Waterloo
- Institute for Security, Privacy and Information Assurance, University of Calgary
- Centre for Cybersecurity, Concordia University
- Canadian Institute for Cybersecurity, University of New Brunswick
- Rogers Cybersecure Catalyst, Toronto Metropolitan University

The initial objectives of this network were:

- Consolidate all cybersecurity and privacy related research expertise in Canada through one hub
- Facilitate academic, industry, government, and international collaborations
- Respond to government program and policy announcements and requests

In anticipation of ISED's announcement for the formation of a cybersecurity network and \$80 million worth of funding through CSIN, a collective decision was made to solidify the network into the NCC. The NCC progressed, and was established as a not-for-profit, federally incorporated entity in 2020.

The NCC has relationships with all elements of the Canadian cybersecurity community, built through the activities undertaken by its founding members over many years. These relationships were leveraged to understand the cybersecurity challenges from academic, industrial, and government perspectives. Equipped with this information the NCC's mission and mandate became clear:

Mission: A multidisciplinary network that bridges all cybersecurity and privacy expertise across Canada to empower the Canadian cybersecurity ecosystem.

Objectives: Pursue three pillars of objectives:

- foster and cultivate world-class cybersecurity-related research and innovation
- develop new and up/reskill highly qualified personnel
- accelerate the commercialization of valuable intellectual property into and through industry members

Focus: Five networks work together as equal parts of an integrated network that supports and informs the other's activities. The five networks are:

Network Security

Leads: University of New Brunswick; Concordia University

Purpose: To develop tools, techniques, and procedures to safeguard computer networks and hosts from both internal and external exploits.

Software Security

Leads: University of Waterloo; Toronto Metropolitan University

Purpose: To develop tools, methods, and practices to reveal and cure vulnerabilities before software is released to end-users.

Privacy

Leads: University of Calgary; University of Waterloo

Purpose: To develop privacy-protective technologies across many different environments that protect individuals and data from likely privacy violations.

Critical Infrastructure Protection

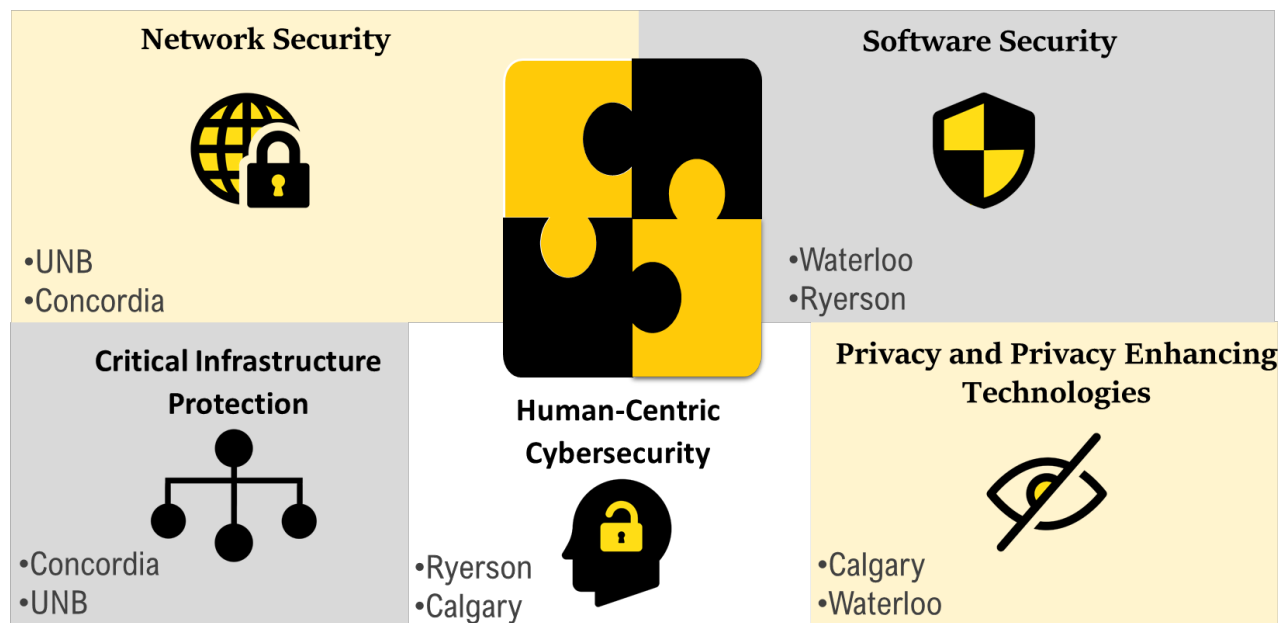
Leads: Concordia University; University of New Brunswick

Purpose: To develop solutions that enable proactive monitoring and real-time detection to mitigate and restore CIs from damage and interruptions inflicted by cyber-attacks.

Human-Centric Cybersecurity

Leads: Toronto Metropolitan University; University of Calgary

Purpose: To understand human factors in respect of security and privacy requirements and propose new cybersecurity techniques to address these human factors.



Growth

Throughout late 2020 and 2021, CPI staff and the Office of Research at the University of Waterloo began to build the NCC's first private and not-for-profit sector memberships. Colin Russell, managing director of CPI and manager corporate research partnerships of the office of research, worked closely with Krista Hrin, operations manager of CPI, and Florian Kerschbaum to begin a large outreach campaign. The inception of the outreach campaign by CPI pre-dated that of the other founding partners by over 8 months.

Marketing materials and outreach strategies were drafted and conceived by CPI that spoke to every sector of Canadian business. The goal was not only draw attention and membership to the NCC, but to also advocate for the importance of cybersecurity and privacy to all sectors of business. It quickly became apparent that the advocacy component of the outreach was, disappointingly, a hallmark of conversations with businesses in many sectors.

The lessons learned throughout 2020 and 2021 would go on to inform how the other founding academic partners of the NCC would recruit further private and not-for-profit sector partners. Indeed, CPI was so far ahead of the other partners in private and not-for-profit sector recruitment that CPI's managing director, Colin Russell, would be nominated to lead the business development committee of the NCC in 2021. Further, the marketing materials created in 2020 would form the basis for the committee's outreach.

By the time of submission to ISED's CSIN program the NCC grew from a small group of 5 academic institutes and centres to fielding a membership of 122 participating organizations across Canada, including:

- 42 post-secondary institutions – with a combined 140 researchers
- 16 large companies
- 30 small and medium-sized companies
- 26 not-for-profit organizations
- 8 governments/governmental agencies

Private and not-for-profit sector members found value in the objectives of the NCC (i.e., R&D, Commercialization, and Talent/Upskilling) and provided commitments to leverage funding in anticipation that ISED would award the CSIN program to NCC. Indeed, through the business development activities led by CPI, 78 proposals were identified as potential projects that can be implemented in the first year of operations, including 17 in commercialization, 31 in training, and 30 in research and development. Combined through these projects and other member commitments the NCC secured over \$55 million in cash and \$102 million in in-kind support to begin leveraging the \$80 million from the CSIN program. It is expected that a significant portion of the proposals in R&D and talent/upskilling will flow through CPI and its members.

Current and Future Activities

The NCC will drive critical benefits for the Canadian cybersecurity ecosystem and Canada in general through: increased cutting-edge IP generated by Canadian cybersecurity researchers (Pillar #1 R&D), effectively commercialized into new products and services by well-supported Canadian SMEs and large enterprises (Pillar #2 Commercialization), and operationalized by a growing, increasingly diverse, and well-trained cybersecurity workforce (Pillar #3 Talent/Upskilling). The NCC is uniquely capable of swiftly implementing this vision through its deep existing involvement in the Canadian cybersecurity ecosystem, as demonstrated by the support the NCC has generated for the program.

CPI will play a key role in the success of Pillars #1 and #3 for the NCC. Within these research pillars, CPI is strongly positioned to lead the software security and privacy networks of the NCC. Indeed, CPI members are ranked #3 in the world, #2 in North America for data security and privacy research, and ranked #10 in the world, #7 in North America for software security research.

Further, WatSPEED – a new business unit within UWaterloo - will be the vehicle through which CPI and the NCC will partner for pillar #3. WatSPEED provides professional education designed as a new approach to lifelong learning, helping the leaders of today and tomorrow navigate an ever-changing professional environment. CPI members are already piloting these micro-credential courses and are looking to expand these offerings to support the talent pipeline for Canada.

Pillar #1 R&D Leadership in Software Security and Privacy Networks:

Software Security

According to figures provided by data specialist firm Advisen, there were almost **5,000** successful cyber-attacks in the global financial sector from 2014 to 2018. These attacks affected over **550 million** records,

with known direct losses of more than **\$4 billion**. 2019 was the worst year for attacks in Canadian history. With software being an essential component of every Canadian's life, especially with millions of them working from home in 2020, it is more important now to secure the software that they depend on. CPI brings together researchers in the following sub-themes that will help secure the various aspects of software:

Secure System Design

Secure System Design is concerned with the invention and codification of software designs, as well as software development methodologies that have been shown to promote the security and privacy of software systems. The growing prominence of massively distributed and pervasive computing has given rise to unique security- and privacy-related research challenges and knowledge gaps in three system categories: (a) the Internet of Things (aka cyber-physical systems), (b) pervasively deployed end-user systems such as mobile applications, and (c) cloud-based software systems. There are also cross-cutting research topics that promote the security and privacy of software systems in all of the three above-mentioned categories. These include the codification of best practices, the design of advanced access control and data governance models, and the design of Artificial Intelligence-based systems.

Program Analysis/Formal Methods/Defensive Programming

Programming languages are the instruments through which software developers transform their ideas into products. The security and safety of these products is primarily determined by the available program analyses, formal methods, and verification tools that support the software developers. Existing approaches do not scale to real-world codebases, produce too many false positives, or do not integrate well into the development environment. To overcome these limitations, we plan to design a suite of program analyses that are of fundamental importance to cybersecurity, such as analysis of access-control policies, information flow security, regression verification, and hybrid analysis approaches, as well as developing better tool integrations and visualizations for domain-specific languages and for general-purpose programming languages, such as C/C++, Java, and Swift.

Mobile and Web Application Security

In the sub-theme "Mobile and Web Application Security", we have identified the following gaps; several open problems still exist in the automated evaluation and test of mobile and web applications for security. These are due to, e.g., the complexity of the applications, the technological landscape, or the opportunities for new attack vectors. User and device authentication is still problematic, and often prone to privacy issues. Cryptographic key management for securing app installation and updates, and the use of hardware features to enhance security, are also areas ripe for breakthroughs. Finally, we still have many open problems concerning the detection of, and the protection against, malicious behavior and cybercrime, in particular when it comes to industry-scalable solutions and 0-victim detection.

Platform Security

This sub-theme centres on security problems of the low-level portion of computing systems, including but not limited to; hardware, firmware, and operating systems, which are more trusted and perceived as trustworthy. Identified gaps and challenges therein include: how to have the low-level better reflect high-level semantics, how to bring high-level mechanisms down to low-level for hardened enforcement, how to anchor trust in a traditionally untrusted context, and how to bridge the gap between the assumed trust and the actual low-level insecurity.

Malware

The undeniable growth of overly connected and AI-driven software and hardware systems irreversibly transformed the threat landscape. AI-enabled systems pose many challenges. The new deployments face increasingly adversarial environments that are unpredictable in nature and consequently vulnerable to unknown malware attacks. On the other hand, adversaries leverage AI benefits creating stealthy, adaptive, destructive, and constantly evolving malware that evades our traditional defenses emphasizing the dire need

for innovative approaches to the problem. The research will focus on three grand challenges: **(1)** innovative malware analysis toolchain capable of uncovering and analyzing newly emergent malware, **(2)** malware for emerging IoT platforms and low-level hardware components, and **(3)** AI-driven malware.

Privacy

The area of research centered around privacy is organized around five themes, each composed of interrelated challenges and objectives. These themes collectively form a holistic approach to address issues associated with cyberprivacy and data security that both threaten Canadian enterprises and allow for marketing opportunities wherein Canada can export its expertise through resulting products and innovations.

Human Communications

Economy & Government: this theme focuses on the challenges that arise where technology and social activities, systems and functions integrate. The necessity to develop digital forms of economic activities and the need to provide virtual government services must ensure privacy and confidentiality by understanding various risks including vulnerabilities, behavioural analysis, and the use of data collected to profile people, or commoditize personal information. Specific aspects to be investigated include mobile app privacy, workplace and in-home surveillance, telehealth service delivery, enhancing consumer privacy, use of encryption including within political elections, and the impacts of privacy on global economic activities. Regulatory and governance issues are a cross-cutting theme impacting on each of these opportunities and risks.

Monitoring/Surveillance and the Internet-of-Things (IoT)

Increasing numbers and types of devices (e.g., computers, microphones, speakers, utility meters, switches, medical devices, smartphones, appliances, televisions, drones, security systems, tablets, digital assistants) are becoming connected to the Internet. IoT has emerged as a new paradigm of computation and data processing at a massive scale. The proliferation of GPS-enabled smartphones and personal AI assistants have also contributed significantly to the adoption of IoT in the personal spheres of our lives. Research will address current societal challenges in cybersecurity and privacy in light of IoT and related trends. We will focus on three key issues of our increasingly monitored society: namely, **(i)** ubiquity, **(ii)** developing enhanced sensors for security and privacy, and **(iii)** a targeted study of security and privacy issues when using sensors for health and community well-being.

Privacy and Artificial Intelligence

AI is both a tool to enhance privacy and a threat to privacy. The privacy network will address both aspects of this dichotomy. The Deep Learning revolution coupled with Big Data has enabled a “quantum leap” in the prediction power in many domains, which has led to the possibility to realize inferences with an unprecedented level of accuracy and detail. The success of machine learning models is such that they are now ubiquitous in our society, which poses an existential threat to privacy. Conversely, AI can protect privacy by ensuring that the privacy preferences of people can be respected in dynamic and diverse environments that would overwhelm people if constant interactions were required to provide permissions.

This theme addresses: **(1)** the privacy risks associated with machine learning models and how they can be mitigated; **(2)** building machine learning models in a privacy-preserving manner; **(3)** leveraging machine learning to contribute to privacy protection; and **(4)** examining existing and emerging legal and normative approaches to AI. Policy, technology, education, human communications, economy, government monitoring, surveillance, AI/ML/DM decentralized management, instruments computation, and communication infrastructure, recommend measures to protect privacy and to ensure the ethical, accountable, and transparent development of AI-based systems.

Decentralized Management and Instruments

Centralized data repositories have traditionally been the approach to collection, storage, and processing of personal information. This approach places substantial responsibility on the collector to behave ethically and requires substantial trust; this has not always occurred. Companies and governments are investigating “decentralized” technologies for finance, data tracking, and identity using various novel tools or instruments. One such technology is blockchain, which has been proposed to address privacy concerns in areas such as finance, health, and private and not-for-profit data. Decentralized technologies allow the individual to control access to and the use of their individual data. These technologies also provide an auditable history of how and why data has been accessed. Areas of investigation include verifiable banking, electronic medical records, and personal identity information that can verify characteristics such as age or vaccination status without revealing specific personal information.

Computation and Communication Infrastructure

A broad range of technical challenges must be addressed to enable individuals and organizations to achieve a high level of privacy protection. Protection from inappropriate digital surveillance, through to empowering organizations to undertake novel data-driven objectives within the bounds of privacy legislation, can only be realized by addressing fundamental scientific questions. Cryptographic primitives, protocols, and infrastructure form a technological basis for privacy; understanding the impact of nascent technologies such as quantum computing are essential to affording protection. Fundamental work to query over encrypted data will allow for stronger methods to protect data even in the event of data breaches. Issues around the appropriate management and use of meta-data that can lead to inference attacks outside of access to the specific data is also addressed in this theme.

Training and Education

Across all these themes there is a need to develop expertise capable of addressing the various privacy challenges. In addition to developing the highly trained personnel required to do the fundamental research and then to bring that knowledge to the marketplace, there is a clear need to educate the public, government, and industry in the importance of these issues; the threats they pose, and the opportunities they present for innovation and entrepreneurial activities, both nationally and internationally. It is also important to note that the growing need for experts in this area offers opportunities for current practicing professionals across all disciplines to acquire expertise in these areas, thereby allowing for diversification of our existing workforce into an area of high need and with a bright future.

Pillar #3 Leadership in Talent & Up/Reskilling:

The NCC’s objective in driving the growth and diversity of the cyber security work force in Canada is to address the two serious and related challenges in the Canadian cybersecurity labour market: **1)** lack of specific skills to address cybersecurity industry labour needs; and **2)** the serious lack of diversity in the sector, with far too few women and BIPOC cybersecurity professionals.

To meet these challenges, CPI and WatSPEED will work together to develop and offer cybersecurity micro-credential courses in partnership with NCC and its private, not-for-profit, and government sector members. These partnerships will develop programs that demonstrate both **(1)** integrated collaboration between training entities and employers, and **(2)** substantial effort in delivering the training programming to women and under-represented demographic groups.

In respect of collaboration between training entities and the employing organizations, the cyber security field calls for the rapid and agile development of training programming that integrates the unfolding requirements of employers in the field. Trained personnel must be ready to contribute actively to their

employers immediately, without additional extensive training. To achieve this, employers must be involved to a significant extent in the design phases of training programs.

Appendix C Membership Survey

This [questionnaire](#), whilst still open to report, has yielded 25 responses from the CPI membership as of Sep. 22/2022. This summary is intended to highlight the dominant themes within the responses, and pair them with recommendations for future initiatives based on these findings.

Questions asked in the survey relevant to feedback:

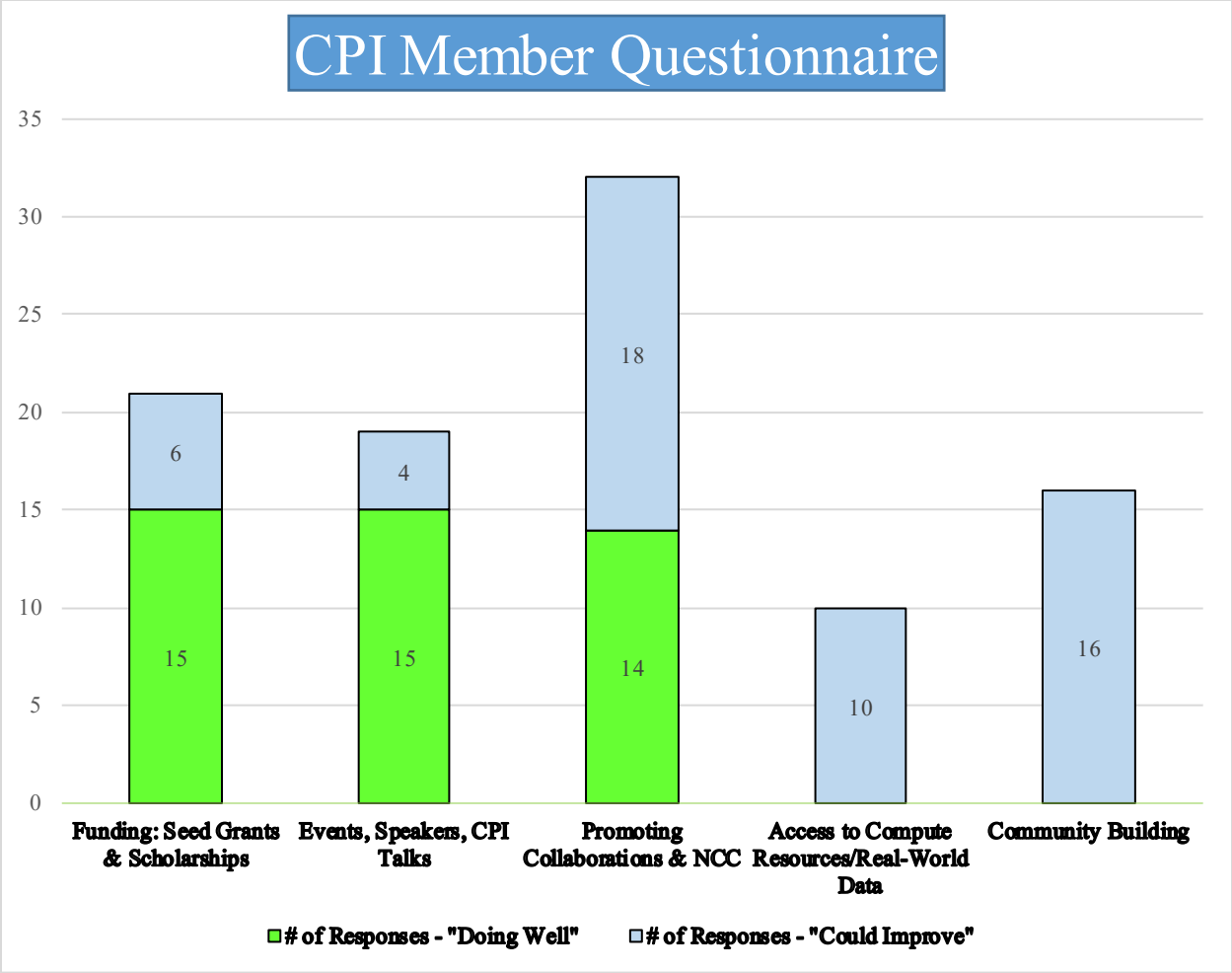
- What has CPI been doing well?
- What can CPI do better?

In the first section, the question posed was, “What is CPI doing well?”, and the second section queried, “What can CPI do better?”. The survey itself was comprised of 4 questions; the benefit to brief surveys is that people respond quickly, and provide the answers that come to mind first, these generally being the most significant to them. This is the ‘first thought/best thought’ model.

In reference to how the CPI membership expressed their interests, three dominant themes emerged, and rather convincingly so. Primarily, CPI members are both positively inclined towards and most interested in Seed Grants and scholarships, followed closely by our media events and speaker series (inc. CPI Talks), and finally with a trend towards industry/collaborations and engagement with the NCC. Whilst it is not surprising that CPI members appreciate financial support, it is noteworthy that they agree on the importance of Seed Grants, as well as scholarships. Clearly, the current framework for Seed Grants should be discussed and reviewed with our membership, in an effort to determine how we might refine or bolster their implementation.

Notably, the responses to both questions evidenced a very strong positive trend towards media events and community building. These two concepts should be linked together, as they both involve creating a stronger and more coherent public image that is based on shared interests and collaborative efforts. Opinions were expressed that centered on there being a demonstrable need for CPI to be more publicly visible across multiple venues in aid of multiple benefits, including professional reputation for the University of Waterloo and CPI, involvement with the NCC, as well as industry and research collaborations.

Moreover, that the CPI membership believes that there is a perceived need for greater cohesion amongst its members, again focusing on collaborative possibilities, awareness of the work and industry engagements that are at play, and with a pointed human element; people would like to feel that CPI is a community of individuals, not just a list of publications beside an email address. This would also add support to the graduate student community, as many of them are no doubt struggling with the responsibilities of their studies and commitments in a pandemic-exacerbated dynamic. The NCC was repeatedly mentioned as an entity of interest, CPI members are invested in the significance that the NCC represents. Finally, the issue of access to compute resources/Chippie cluster (Section 7.1.2) and real-world data was fore fronted as being a desirable outcome.



Appendix D Policy Facing Achievements

In addition to its individual speaker series, CPI Talks, CPI members have taken the initiative to organize large conferences with significant policy ramifications that have attracted substantial attendance by government employees and individuals engaged in public policy.

- Employing CPI and CrySP funding, Jennifer Whitson and Ian Goldberg organized a [one-day event on Privacy and Policy](#) bringing together researchers and international speakers from journalism, national security, academia, and the corporate world to challenge the notion that protecting individual security and privacy involves significant trade-offs. This event was held on Feb 28th, 2020. A central thread of each of the talks was the design, implementation, and benefits of privacy-enhancing social and technological infrastructures. The event had over 100 attendees and included several distinguished speakers such as:
 - Scott Millar, Deputy Chief, Policy and Communications, Communications Security Establishment (CSE)
 - Julia Angwin, Editor-in-Chief and Founder, The Markup
 - Cat Coode, Founder, Binary Tattoo

- Anindya Sen organized a [virtual conference](#) funded by CPI which collected some of the leading COVID-19 policy researchers in Canada to discuss a variety of issues and help frame policy recommendations for different societal issues that have emerged with COVID-19. There are three broad themes:
 - downloads of the Federal Government exposure notification app have been extremely low, mitigating its usefulness. What can be done legally and from a behavioural lens in order to increase the use of exposure notification apps?
 - the lack of disaggregated COVID-19 data across the country has impaired the ability of researchers to conduct relevant and important research. What do governments need to do to ensure better data availability and what are novel data sources that can be studied by researchers?
 - the use of statistical models in predicting the incidence and burden of COVID-19

The conference had roughly 125 attendees. All the papers were collected in an e-book and distributed to policymakers.

The speakers of the conference were:

- Michael Wolfson, University of Ottawa, Former Assistant Chief Statistician, Analysis and Development at Statistics Canada & Adjunct Professor, School of Epidemiology and Public Health, University of Ottawa
 - Colleen Flood, University of Ottawa, Professor, Faculty of Law, University of Ottawa and University Research Chair in Health Law and Policy. Director for the University of Ottawa Centre for Health Law, Policy, and Ethics
 - Anindya Sen, University of Waterloo, Professor of Economics & Director, Master of Public Service, University of Waterloo. Member, Waterloo Artificial Intelligence Institute & Waterloo Cybersecurity & Privacy Institute
 - Jeff Chan, Wilfrid Laurier University, Assistant Professor, Department of Economics, Wilfrid Laurier University
 - Igor Grossmann, University of Waterloo, Associate Professor of Psychology & Director, Wisdom and Culture Lab, University of Waterloo
 - Mark Crowley, University of Waterloo, Assistant Professor, Department of Electrical and Computer Engineering, Waterloo Artificial Intelligence Institute, University of Waterloo
 - Plinio Morita, University of Waterloo, Assistant Professor, School of Public Health and Health Systems J.W. Graham Information Technology Emerging Leader Chair in Applied Health Informatics Director, Ubiquitous Health Technology Lab (UbiLab), University of Waterloo
 - Ashley Rose Mehlenbacher, University of Waterloo, Associate Professor specializing in rhetorical theory and science communication and PI of the Democratization through Education in Medicine, Technology, and Science Lab (Demos Lab)
 - Scott Leatherdale, University of Waterloo, University Research Chair and Professor, School of Public Health and Health Systems, University of Waterloo
 - Ashleigh Tuite, University of Toronto. Assistant Professor of Epidemiology, Dalla Lana School of Public Health, University of Toronto
- Anindya Sen organized a half-day workshop that investigated the effects of cybersecurity regulation and relevant gaps on public policy. Florian Kerschbaum, then CPI Director, made a presentation, as did Anindya Sen. There were several attendees from the Federal Government who attended, including Paul Thompson who was then Associate Deputy Minister of

Innovation, Science, and Economic Development Canada and Joanne Khouryati, Director General, Innovation Canada

- Anindya Sen represented the University of Waterloo in facilitating a presentation on privacy regulation and individual data in Canada to Daniel Therrien, the Privacy Commissioner of Canada
- Through connections facilitated by CPI, W. Alec Cram and Ian McKillop are working on a cybersecurity related year-long research and consulting project with a large provincial ministry that is expected to yield several high-quality research publications
- CPI organized a conference related to contact tracing apps, specifically called [Managing the Pandemic through Contact-Tracing Apps: Technological innovation or a Challenge to Privacy and Civil Liberties](#). CPI speakers who participated included:
 - Florian Kerschbaum (MATH/CS)
 - Douglas Stebila (MATH/C&O)
 - Plinio Morita (HEA/HLTH)
 - Bessma Momani (ARTS/PSCI)

Appendix E Early Career Researchers - Support Letters

Sept 23, 2022

To Whom it May Concern:

RE: CPI Renewal

I am an Associate Professor in the Department of Sociology and Legal Studies and am cross appointed to the Stratford School of Interaction Design and Business. While much of my research lies outside of CPI's mandate, networks developed through the CPI have made me a more skilled researcher, graduate supervisor, and instructor.

One of the most fulfilling parts of my research career have been my collaborations with Ian Goldberg at the Cheriton School of Computer Science. The CPI Seed Grant for the conference was our first collaboration together. This was an in-person event - one of the last before COVID lockdowns. Speakers included Pulitzer-prize winning journalist Julia Angwin and Scott Millar, Deputy Chief, Policy and Communications at Communications Security Establishment (CSE). Along with a full slate of speakers, we hosted graduate student speaker talks and poster sessions. Five of the speaker talks can be viewed here: <https://crysp.uwaterloo.ca/speakers/>.

Since then, Ian and I have worked on community projects together, given research talks together and taught together in 2020. Part of this collaboration also includes inviting and hosting speakers that, on its own, the Sociology and Legal Studies Department simply wouldn't have the resources to support. This includes David Murakami Wood, Val Steeves, Safiya Noble, Alex Rosenblatt, etc. While not directly supported by the CPI, CPI helped build the cross-faculty networks that "seeded" these bridging dialogues and opportunities.

Without the initial funded collaboration, Ian and I would likely not have taken the risk of teaching together. SOC 701/CS 858 was, as far as I'm aware, the first co-taught course at Waterloo to be offered between Sociology and Legal and Studies and Computer Science. The course focused on Surveillance and Privacy Enhancing Technologies, and attracted students from Computer Science, Sociology, Political Science, Global Governance, English, Systems Design Engineering, and Applied Health Science, as well as faculty auditors in Optometry and Computer Science. It was a delight that we hope to do again, particularly given that I still cite some of the student projects.

Beyond facilitating research and teaching collaborations like I have with Ian, the other central role of the CPI is in providing resources and a network that assists our department in recruiting top talent. Colin Hastings and Adam Molnar joined the CPI



immediately upon arrival. The availability of seed grants and research collaborators from other faculties is valuable for both recruiting and helping our faculty hit the ground running as they join UW and build research capacity. Currently, our department has the greatest hub of surveillance studies researchers in Canada.

CPI grants have also supported my graduate students, Brian Schram and Krystle Shore, and provided a venue for their work, both at the CPI Annual Conference and online. For example, the CPI funded the creation of a video promoting grad student Brian Schram's diss project. This video (<https://vimeo.com/250528017>) was useful as public knowledge mobilization and was re-used by the Faculty of Arts in their social media recruiting. I also happened to use in an undergraduate class on Digital Cultures just this week.

CPI supports all of this.

Sincerely,



Jennifer R. Whitson, PhD

Associate Professor

Sociology and Legal Studies / Stratford School of Interaction Design and Business

University of Waterloo

www.jenniferwhitson.com

email: jwhitson@uwaterloo.ca



August 23, 2022

Dear Sir/Madam,

I am writing to express my gratitude and support for the Cybersecurity and Privacy Institute (CPI) at the University of Waterloo. I have been a member of the CPI since 2018 after I joined Waterloo as a Lecturer. In my current position as Assistant Professor, my research aims to understand and improve people's digital experiences, knowledge, and technology practices, focusing on computer security, online privacy, and digital literacy.

The CPI provided research funding, collaboration and network working opportunities and supported knowledge mobilization initiatives. For example, in 2020, the CPI Seed Grant funded the uXperience | Think Privacy Design Jam at the Stratford School of Interaction Design and Business. The CPI funding was used to support industry professionals and academic researchers to provide workshops, presentations, and mentorship that helped students acquire the knowledge and skills to create privacy-aware solutions, regardless of their background and experience. The contribution of the CPI is threefold. First, the institute helped promote the importance of interdisciplinary collaboration in creating privacy solutions. Second, the funding provided valuable networking opportunities between the Stratford School and CPI's network of researchers, industry professionals, and entrepreneurs. Third, the event introduced many university students to cybersecurity and privacy as potential career paths.

In 2021-2023, the CPI Seed Grant funded my research project titled "Secure Software Development." The work aimed to understand the context in which developers produce security-relevant code and provide tools and processes that better support both developers and secure code production. The seed funding enabled me to conduct an initial investigation of a larger research objective, which built the foundation that partly led to the success of my 2022 NSERC Discovery Grant.

I am pleased to give back to the CPI community by serving on the 2022 CPI Seed Grant evaluation community. I expect the funded research proposals will lead to several significant contributions and research collaborations between faculty members from different departments at Waterloo.

Sincerely,

Leah Zhang-Kennedy



Assistant Professor, Interaction Design and User Experience Research
Stratford School of Interaction Design and Business
University of Waterloo





UNIVERSITY OF WATERLOO
FACULTY OF ARTS
School of Accounting and Finance

W. Alec Cram
Associate Professor

519-888-4567 x48060
wacram@uwaterloo.ca

289G Hagey Hall
200 University Ave W.
Waterloo ON N2L 3G1

August 19, 2022

To whom it may concern,

I am writing to express my strong support for the ongoing activities of the Cybersecurity and Privacy Institute (CPI) at the University of Waterloo. In my current role as an Associate Professor at the School of Accounting and Finance, I conduct research in behavioural aspects of cybersecurity, including issues such as why employees comply with or violate organizational policies. I have been a member of the CPI since 2019, when I joined the University of Waterloo.

My view is that the CPI provides a critical role as a central hub of cybersecurity activity at the University. Over the past year, I have been contacted by the CPI in regard to several promising opportunities to connect with organizations that require cybersecurity expertise, as well as ongoing developments with cybersecurity teaching. In particular, the connection with practitioners is often difficult to come by, but the CPI is in an ideal position to act as an intermediary to connect interested organizations with specialists at the University. In one of the cases, the opportunity has matured into a year-long research and consulting project with a large provincial ministry that has engaged myself, another UW faculty member (Dr. Ian McKillop), and an SAF doctoral student. I expect that several high-quality research publications will result from the initiative. We would not have been able to undertake this work without the support of the CPI and I am most grateful for their support.

Further, over the past three years, I have served on the evaluation committee that awards the annual CPI Excellence Graduate Scholarship. The strength of applications has been very high each year and I believe the CPI is fulfilling a valuable service by allocating these scholarships to talented students at the institution.

Please feel free to reach out to me at any time should you require any additional information.

Sincerely,

A handwritten signature in black ink, appearing to be 'W. Alec Cram'.

W. Alec Cram, PhD, CISA, CISSP
Associate Professor and PwC Fellow
School of Accounting and Finance
University of Waterloo

August 27, 2022

To Whom It May Concern:

I am writing to express my strong support for the ongoing activities of the Cybersecurity and Privacy Institute (CPI) at the University of Waterloo. I am currently an Assistant Professor at the Department of Computer Science, the University of Waterloo. My research focuses on privacy and security for big data, including developing usable and trustworthy tools for data exploration and machine learning with provable security and privacy guarantees. I have been a member of the CPI since 2019 when I joined the University of Waterloo.

With the vision to become a leading interdisciplinary research institute in cybersecurity and privacy, the CPI has made vital initiatives and built resources to drive critical research in these areas. First, the institute has actively engaged Waterloo's expertise in diverse areas, including computer science, engineering, mathematics, cryptography, and quantum computing, with companies through workshops and seminars such as CPI talks, CPI Spotlights, and CIP RoundTables. Our research group, including my students and myself, has benefited from presenting our research and attending the talks. In particular, we presented our work on APEX for differentially private data exploration in one of the seminars to the industrial partners of CPI, who later shared with us several practical use cases to apply our technologies.

Through CPI's connections with the industry, we have also initialized collaboration with the team at Source Inc on a research proposal, "Scaling Oblivious Query Processing using Differentially Private Indexes," in submission to the Ontario Centre of Innovation. We expect novel prototypes to be developed with our industrial partner and a few high-quality publications from this collaboration. In addition, the CIP provides its members and their sponsored students with reliable computing and generous financial support. For example, our research project, CacheDP, a recent submission to a top database conference venue, was fully developed and tested using the Chippie Cluster, a computing cluster provided by the CPI. At one of the CPI annual events sponsored by Symcor, my student received the best poster award for his master thesis on "differentially private learning with noisy labels."

Overall, the CPI's presence at the University has played a critical role in recognizing the excellent work of Waterloo's researchers, identifying industrial collaborations, and bringing knowledge on cybersecurity and privacy to practical applications. I would like to give my full support in the renewal process of the CPI. Please feel free to reach out to me at any time should you require any additional information.

Sincerely,



Xi He
Assistant Professor
Department of Computer Science
University of Waterloo
Web: <https://cs.uwaterloo.ca/~xihe/>
Email: xi.he@uwaterloo.ca





August 25, 2022

Meng Xu
Assistant Professor
200 University Ave W
Waterloo, ON, N2L 3G1
Phone: [REDACTED]
Email: meng.xu.cs@uwaterloo.ca

To whom it may concern,

I am writing this letter to express my strong support for the ongoing activities and future initiatives of the Cybersecurity and Privacy Institute (CPI) at the University of Waterloo. I am an Assistant Professor at the Cheriton School of Computer Science and my research mainly focuses on software and system security, including automated program analysis, testing, and verification. I have been a member of the CPI since September 2021, immediately after I join the university.

My interaction with CPI for the past year has led me to believe that CPI has become a central hub of cybersecurity-related activities at the university, and serves as a single-point of contact on cybersecurity affairs both internally to other departments of the university and externally to the public. This is evident on both missions of CPI: nurturing cutting-edge research and boosting cybersecurity training and awareness.

On the research side, I am mostly grateful to the various forms of support CPI offers, especially as an early-career faculty member. I have been invited to three round-table discussions with both university institutions (RoboHub), and industrial partners (BlackBerry and EPAM). Through these discussions, I made the initial contact to many potential collaborators and was offered channels and support to apply for both CPI seed funding as well as external funding (e.g., from NSERC). Out of these discussions, at least one will mature into a multi-year funding. Besides the initial liaison support, CPI also provides consistent support for ongoing research. In particular, the Chippie cluster features a fleet of many-core high-memory machines that meet the parallelization requirement for my research work. The annual poster session provides an opportunity where my student and I can advertise our ongoing research and source for early feedbacks.

On the cybersecurity training side, my view is that CPI is determined to address the significant shortage of skilled cybersecurity professionals. I co-instructed CS458 - Computer Security and Privacy in the Winter 2022 term and co-piloted the first CPI Undergraduate Award — a cash award of \$1,000 for the top-performer of this course. Despite the chaotic return-to-campus situation in that term, this scholarship indeed boosted the students' in-class participation and interests in tackling cybersecurity-related issues. I have also been invited to several discussions on cybersecurity training hosted by CPI, for both the National Cybersecurity Consortium (NCC) and the Master in Cybersecurity and Privacy program, and I look forward to my future participation in the construction of a WatSPEED cybersecurity certificate program.

In summary, I am extremely satisfied with my experience at CPI and I look forward to the future initiatives from CPI. Please feel free to reach out to me at any time should you require any additional information.

Sincerely yours,

Meng Xu

Appendix F Support Letters

Letters from CPI members



Arie Gurfinkel
Professor
Electrical and Computer Engineering
University of Waterloo
Phone: +1 (519) 888-4567 x36616
Email: arie.gurfinkel@uwaterloo.ca

September 9, 2022

To whome it may concern,

I am delighted to write this letter to express my strong support for the ongoing activities and future initiatives of the Cybersecurity and Privacy Institute (CPI) at the University of Waterloo. I am Professor at the Department of Electrical and Computer Engineering at the University of Waterloo. My research is primarily in the areas of Program Verification, Automated Reasoning and Model Checking. In recent decade, the primary application of my research has been in the area of cybersecurity, specifically, ensuring trust in low-level code through automated verification. I joined CPI in October of 2018 to widen my collaboration opportunities within the University.

CPI is a centre for cybersecurity and privacy research at the University. It provides an invaluable service in connecting researchers, industry, and the public. Many of its public activities such as the CPI Talks, CPI Spotlights, and CPI Roundtables are essential and disseminating awareness of cybersecurity and privacy in general, and awareness of the current research conducted by University of Waterloo faculty in particular. CPI internal activities nurture and facilitate research through interaction with industry, internal funding opportunities, and scholarships for graduate students.

I have personally benefited tremendously through my interactions with the CPI. I hold a multi-year NSERC CRD grant that was facilitated by the interactions administered by the CPI. My students have participated and presented at the annual CPI conference. These presentations have grown into new collaborations with faculty across the university, and potential collaboration opportunities with industry. Finally, one of my PhD students is supported by the CPI Graduate Scholarship. For the student, this is an important financial incentive. However, perhaps more importantly, it is recognition and validation of his research that is very important that early in his academic career.

In conclusion, I want to reiterate my strong support for the CPI. It is a wonderful and fruitful initiative. I am looking forward to contributing to its growth and benefiting from the opportunities it provides. Please feel free to contact me for any additional information.

Sincerely,

Prof. Arie Gurfinkel



Letters from Deans

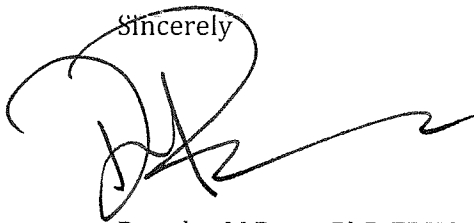
16 August 2022

Dr Charmaine Dean
Vice-President Research and Innovation

Dear Dr Dean

On behalf of the Faculty of Arts, I am delighted to offer this letter in support of the renewal of the Cybersecurity and Privacy Institute. Over the course of its relatively short history, CPI has brought together an impressive range of scholars from across campus around some of the most pressing challenges facing our increasingly interconnected and digitized society. In so doing, CPI plays a vital role in the University of Waterloo's stated goal of 'Advancing Research for Global Impact' by creating not only a space but also opportunities for researchers from diverse backgrounds to collaborate in fruitful and innovative ways. Like so many of the wicked problems facing society today, issues of cybersecurity and privacy are best addressed by exploring the interstices of technology, society, and policy, and the CPI is well positioned to serve as a catalyst. To date, twelve members of the Faculty of Arts have joined in its activities and I foresee that number increasing as the breadth of its activities grow. It has already contributed to a number of major collaborative and institutional grants and has provided the foundation for several more that are underway. By mobilizing researchers from across campus, CPI serves the purpose for which institutes are designed: fostering interdisciplinarity within an increasingly specialized world.

Sincerely



Douglas M Peers PhD FRHS
Acting Dean of Arts
Professor of History



October 28, 2022

Senate Graduate and Research Council University of Waterloo

Re: Letter of Support for the renewal of the Cybersecurity and Privacy Institute (CPI)

Dear SGRC,

The Faculty of Engineering enthusiastically supports renewing the University of Waterloo's Cybersecurity and Privacy Institute (CPI).

Cybersecurity is a field of research that examines ways to protect the digital interests of people, households, companies, cities and nations. Our data and digital devices are more vulnerable than ever due to the vast amount of sensitive information stored not just digitally but on networked systems and the connected devices that make up the Internet of Things (IoT).

The University of Waterloo has unparalleled multidisciplinary breadth in cybersecurity and privacy, allowing it to both understand and confront core cybersecurity and privacy challenges in different application areas including engineering, healthcare, financial and other sectors, and to be able to do so through an interdisciplinary approach covering technological, social, economic, and policy aspects

CPI's continued vision is to build on the outstanding reputation of the University of Waterloo and its strong history of entrepreneurship and partnership. CPI holds a unique position in advancing the research frontiers and effective delivery of cybersecurity innovation for all segments of our society.

CPI is uniquely suited to strongly represent the University of Waterloo in the global cybersecurity and privacy arena. The renewal of CPI and the continued support of its mission to promote and support cybersecurity and privacy research, training, and raising awareness is a critical contribution to the University of Waterloo's current and emerging strategic goals.

Yours very truly,



Mary Wells, Dean
Faculty of Engineering





19 October 2022

Prof. Charmaine Dean
Vice-President Research and International
University of Waterloo

Dear Prof. Dean,

On behalf of the Faculty of Environment, I enthusiastically offer this letter in support of the renewal of the Cybersecurity and Privacy Institute. The interdisciplinary approach of the Institute to tackling the increasingly complex dimensions of cybersecurity and privacy resonates with the Faculty of Environment's view that a sustainable future is only achievable through broad disciplinary collaboration and cooperation. The CPI is a shining example of how to do this by bringing together a diversity of scholars within the academy (and from the broader society). Waterloo is set to lead this field, both in basic and applied research and policy.

On behalf of our Faculty, we look forward to ongoing and future collaborations with the team at CPI and its broad membership. Cybersecurity and privacy matters are not only the domain of technology but increasingly lie at the centre of ethics, cross-sectoral data gathering and use, law, governance, and the values of freedom of association and expression. The CPI is crucial to the evolution of our collective approaches to living sustainably with technology.

Sincerely,

Bruce Frayne
Dean, Faculty of Envi



15 October 2022

Dr Charmaine Dean, Vice-President – Research and International
Needles Hall

Re: Support for renewal of Waterloo’s Cybersecurity and Privacy Institute

Dear Prof Dean,

The Faculty of Health enthusiastically supports the renewal of the mandate for the University’s Cybersecurity and Privacy Institute.

Matters of privacy are exceptionally relevant to health researchers and health practitioners. Not only does the health sector face unique challenges with respect to privacy, we also work within the confines of legislation that addresses the unique nature of our sector and the information we gather. There is often a difficult tension between the need to ensure the privacy of health information to protect individuals and the need to share information in order to provide quality care. The University of Waterloo’s research capacity in cybersecurity and privacy informs and leverages the expertise of our scientists in the School of Public Health Sciences, Kinesiology and Health Sciences, and Recreation and Leisure Studies.

The solution to privacy challenges is not to enact more complex legislation, as often seems to be the route chosen. Instead, the solution is to find innovative, scientific breakthroughs that ensure all stakeholders can achieve their objectives. The Institute provides a thriving community on campus where these issues can be explored, and

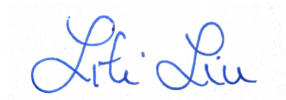


ensures that the unique challenges presented by health data are considered, thereby allowing the University of Waterloo to make vital contributions to this field in the real world.

Equally important to Health researchers are matters of cybersecurity – whether it is to protect the integrity of our research findings or as a core part of our research endeavours. Our Faculty’s thrust into the area of Health Informatics increasingly finds our students and faculty developing technology-based approaches to address important health challenges. No technology-based approach can be successfully implemented if cybersecurity is not well considered. Our researchers are enthusiastic about continuing to contribute to the Cybersecurity and Privacy Institute’s endeavours.

The Faculty of Health recognizes the importance of the role of a university level institute that fosters interdisciplinary collaboration in the cybersecurity and privacy space and heartily endorses the renewal of the Institute’s mandate.

Sincerely,



Lili Liu, PhD, Professor & Dean



July 13, 2022

Charmaine Dean, Vice-President, Research and International
Re: Support of the Waterloo Cybersecurity and Privacy Institute

Dear Professor Dean,

The Faculty of Mathematics enthusiastically supports the renewal of the Waterloo Cybersecurity and Privacy Institute (CPI). This institution is comprised of members from every faculty, allowing a thorough understanding of the broad range of industrial and societal implications of cybersecurity and privacy-related research and technologies. CPI is tackling critical global issues head-on by building on UWaterloo's expertise in security & privacy, cryptography, mathematics, computer science, and quantum computing to create world-leading cybersecurity research and technologies while increasing interdisciplinary collaboration. Cybersecurity, privacy, and data science is identified as one of the key global challenges in the Strategic Plan that UWaterloo is committed to aligning its research strengths with. CPI is uniquely positioned to make immense contributions to this goal.

CPI has established itself as a premier institution and founding member of the National Cybersecurity Consortium (NCC), which works with the public and private sectors to lead world-class cybersecurity innovation and talent development. CPI was one of a select few organizations selected to form the Cyber Security Innovation Network (CSIN) and named the lead recipient of an \$80 million grant to support further research and development, increase commercialization opportunities, and develop skilled cybersecurity talent across Canada.

Based on cybersecurity and privacy research output, CPI researchers' contributions have led to the University of Waterloo being recognized as an international leader with the following rankings:

- #1 in Canada and #14 worldwide in the technology side of cybersecurity and privacy research output
- #3 in North America and #4 worldwide in Data Security and Privacy
- #5 in North America and #7 worldwide in Software Security

In addition to prestigious international contributions and recognition, CPI has established itself as the leader on campus for communication and resources relating to cybersecurity and privacy. Through outreach events for the public, multidisciplinary roundtable discussions, articles highlighting researchers and their contributions, graduate student scholarships, undergraduate awards, seed grants, and workforce training initiatives with WatSPEED, CPI has established itself as an important member of the UWaterloo community.

Understanding cybersecurity, privacy, and its impact is essential for both the University and society at large. Research into this ever-evolving field and a continued commitment to remaining at the forefront of new advancements are crucial to maintaining UWaterloo's status as an innovative and forward-thinking institution. The Faculty of Mathematics believes that the CPI will continue to create opportunities for interdisciplinary research collaborations, partnerships with industry and government, as well as enhancements to current communications and resources for internal audiences. I strongly encourage the Council to recommend the renewal of the Cybersecurity and Privacy Institute.

Yours truly,

Mark

A handwritten signature in blue ink, appearing to read 'Mark Giesbrecht', with a large, stylized flourish at the end.

Dr. Mark Giesbrecht
Dean, Faculty of Mathematics. Professor, David R. Cheriton School of Computer Science
University of Waterloo, Canada

October 19, 2022

Charmaine Dean
Vice-President Research & International
University of Waterloo

Re: CPI renewal

Dear Charmaine:

I am pleased to write this letter in strong support of the renewal of the Cybersecurity and Privacy Institute (CPI) at the University of Waterloo.

As the Dean of Science, I can attest to the critical value of entities being able to conduct and disseminate research with the surety of cybersecurity and privacy measures in place to protect the knowledge and data that research generates. CPI and its researchers are at the vanguard of technological development in protecting the data and infrastructure that the modern world relies upon. The University of Waterloo's Strategic Plan is predicated on developing talent for a complex future, advancing research for global impact, and strengthening sustainable and diverse communities; CPI and its various initiatives strongly focus on these pillars in the cybersecurity and privacy ecosystem.

CPI delivers an important benefit in connecting industry with researchers, as well as engaging with the public. I would point to their CPI Spotlights, CPI Roundtables, and CPI Talks, as being highly informative and effective at increasing awareness of cybersecurity and privacy in general, as well as shining a necessary spotlight on the current research conducted by University of Waterloo faculty specifically. CPI is also to be commended for its slate of endeavors that seek to support and accelerate research through engagements with industry, internal funding opportunities such as their Seed Grants program, and graduate/undergraduate scholarships for UWaterloo students.

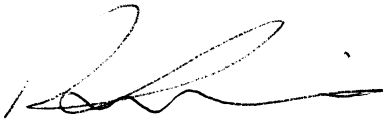
Of significant national note, CPI has proven itself to be at the leading edge of cybersecurity and privacy advocacy as a founding member of the National Cybersecurity Consortium (NCC). The NCC is focused on creating opportunities for cybersecurity innovation and talent development within both the public and private sectors, leading Canada towards world-class standing in these areas. NCC was chosen as the lead recipient for the Cyber Security Innovation Network (CSIN) which is slated to receive nearly \$80 million grant to increase commercialization opportunities, support further research and development, and develop skilled cybersecurity talent throughout Canada.

Finally, I would like to stress that the Faculty of Science acknowledges the critical nature of the activities that CPI nurtures, and I would point to the many ways in which CPI supports its



researchers and creates opportunities for interdisciplinary research collaborations, promotes partnerships with government and industry partners, and strives to raise awareness and engagement with cybersecurity and privacy issues on all fronts. Faculty members and graduate students from the Faculty of Science have been active participants in CPI-led initiatives and benefit from it. I strongly encourage the Council to recommend the renewal of CPI.

Sincerely,



Robert P. Lemieux, PhD
Dean of Science and Professor of Chemistry



Letters from Heads of Academic Units

Regarding the renewal of the Cybersecurity and Privacy Institute

I am very pleased to write in strong support of the renewal of the University of Waterloo Cybersecurity and Privacy Institute (CPI). The CPI serves as a focal point for interdisciplinary privacy and cybersecurity research at the University of Waterloo. CPI provides exceptional financial support for research by way of its seed grant and scholarship funds programs. CPI affiliate members from the Department of Sociology and Legal Studies have had great success converting these funds into very high quality research outputs and knowledge dissemination pieces, including a video production by one of our PhD students on privacy and visibility (available at <https://vimeo.com/250528017>), high quality training for another PhD student leading to an international conference presentation, a conference hosting upwards of 100 academics and practitioners on the theme of public-targeted information tracking, our first team-taught Sociology/Computer Science graduate course focussing on surveillance and privacy enhancing technologies which attracts graduate students from Computer Science, Sociology, Political Science, Global Governance, English, Systems Design Engineering, and Applied Health Science. Our ongoing partnership with the CPI has also enabled our department to recruit top faculty talent to work in the field of technology and society including a Canada Research Chair and two additional faculty with research interests in the social implications of technology.

Given the faculty members involved and the high-quality research and outreach outputs described in the proposal, it is clear that the CPI contributes to the international profile of UW, to our ability to secure research funding and support, and to bring the best researchers in the world to UW. The University of Waterloo is uniquely positioned at the centre of many advanced technological initiatives and developments. The CPI plays a pivotal role in in fostering leading-edge research and far-reaching knowledge dissemination on the some of the most pressing social implications of technological developments. I strongly support the renewal of the Cybersecurity and Privacy Institute.

Sincerely,

Dr. Daniel O'Connor,
Chair, Department of Sociology and Legal Studies,
University of Waterloo

Dr. Charmaine Dean
VP, Research and International
University of Waterloo

August 18, 2022

Letter of Support for the Renewal of the Cybersecurity and Privacy Institute

Dear Dr. Dean,

On behalf of the University of Waterloo Stratford School of Interaction Design and Business, I am writing to express the strongest possible support for the renewal of the Cybersecurity and Privacy Institute (CPI) that was established in 2018 to facilitate collaborative research and training in cybersecurity, and privacy. The CPI's mandate is to provide opportunities for collaborations across the entire University and with companies, research centres, and other institutions in Canada and internationally. Researchers and students at the Stratford School of Interaction Design and Business have benefitted and continue to benefit from the resources the CPI offers.

Specifically, Dr. Leah Zhang-Kennedy has been successful in making significant contributions to cutting-edge research on cybersecurity and privacy thanks to the funding she received from the CPI. In 2021-2023, a CPI Seed Grant funded Zhang-Kennedy's research project titled "Secure Software Development." The work aimed to understand the context in which developers produce security-relevant code and provide tools and processes that better support both developers and secure code production. The seed funding was used to support an initial investigation of a research objective in Zhang-Kennedy's NSERC Discovery Grant proposal, which built the foundation that partly led to the success of Zhang-Kennedy's 2022 NSERC Discovery Grant.

Further, post-secondary students were able to participate in our annual design camp that was funded by a CPI Seed Grant in 2020. The uXperience | Think Privacy Design Jam at the Stratford School of Interaction Design and Business led by Dr. Zhang-Kennedy virtually brought together post-secondary students to explore, collaborate, and propose solutions to address the question: "How might we connect people and create a sense of 'togetherness' while protecting everyone's privacy?" The event theme encouraged creative and novel solutions that address the role and impact of design on people's privacy.



Students worked in small interdisciplinary teams spanning across diverse backgrounds such as interaction design, computer science, engineering, communications, and sociology and legal studies. The CPI funding was used to support industry professionals and academic researchers to provide workshops, presentations, and mentorship that helped students acquire the knowledge and skills to create privacy-aware solutions, regardless of their background and experience. Specifically, the design jam made possible by the CPI had the following contributions:

- Promoted the importance of interdisciplinary collaboration in building a responsible digital future
- Promoted collaboration between the Stratford School and the CPI, and their network of researchers, industry professionals, and entrepreneurs
- Introduced university students to cybersecurity and privacy as potential career paths
- Produced creative solutions to an important problem

I wholeheartedly support the renewal of this important research institute.

Please do not hesitate to contact me directly for further information.

Kind regards,



Dr. Christine McWebb
University of Waterloo Stratford School of Interaction Design and Business
cmcwebb@uwaterlo.ca



Dr. Kankar Bhattacharya, PhD., P.Eng., FIEEE,
Professor & Department Chair,
Department of Electrical & Computer Engineering.

Waterloo, Ontario
September 21, 2022

Dr. Charmaine Dean,
Vice-President Research & International.

Dear Professor Dean,

I am very happy to write this letter, on behalf of the Department of Electrical & Computer Engineering (ECE), to express strong support for a 5-year extension of the University's very innovative and critically important, Cybersecurity & Privacy Institute (CPI). The ECE Department, through several of our faculty members, have been closely associated for many years, with the activities of CPI, and these faculty members have professionally benefitted from this association to further their teaching and research.

In particular, I would like to mention that ECE faculty member, Dr. Vijay Ganesh serves in the Faculty Advisory Committee of CPI. CPI has been helpful in providing funding opportunities to Dr. Arie Gurfinkel with industry through Waterloo Huawei Joint Innovation Lab. It has recognized his students through a Blackberry-funded PhD scholarship and facilitates engagement with industry and other interesting parties through workshop and panel discussions. These have been very helpful in connecting with industry (e.g., Blackberry), and other faculty at UW.

CPI was a founding partner of National Cybersecurity Consortium (<https://ncc-cnc.ca>) which has been named as the lead recipient of an \$80 million grant by ISED to be used to fund research / training / commercialization projects over the next four years. It can be expected that several ECE faculty members (e.g. Dr. Werner Dietl) could benefit from it. Dr. S. Fischmeister has already made a commercialization proposal for the first round. More information is awaited and it is expected that once the NCC program starts up, there will be collaborations with both ECE faculty members and companies.

With regard to student engagements, CPI runs an Excellence Graduate Scholarship program, and as stated earlier, Dr. Gurfinkel's student won it in 2021. I understand that CPI is piloting an undergraduate award program now, to closely engage with undergraduate students. Our undergraduate course *ECE 458: Computer Security*, taught by ECE faculty, Dr. Guang Gong, is part of the pilot, this term, and she has selected a winner from the students of the course, for a \$1000 award.

With regard to faculty engagement, CPI runs a seed grant program to incentivize faculty to bootstrap research and training projects, especially of a multidisciplinary nature, wherein Dr. Ganesh has won the award in the past.

ECE faculty members have been invited to speak at CPI events (for example, Dr. Ganesh, Dr. Fischmeister, Dr. Gebotys have being featured in CPI events). CPI also had web feature on Dr. Gebotys (<https://uwaterloo.ca/cybersecurity-privacy-institute/news/two-uwaterloo-experts-share-six-ways-smash-stem-glass>), while Dr. Gong will be speaking at the upcoming Annual Conference in October.



CPI has helped with grant applications of several ECE faculty members. The Institute has also greatly increased the community building initiatives for members, such as mailing lists, Teams team, internal website, social media presence, a public outreach lecture series (CPI Talks), a CPI researcher Spotlight web article series, and many others.

With these activities, we earnestly hope that it will bring the CPI-affiliated researchers from the ECE Department and other units, closer together and incentivize collaboration. In summary, ECE faculty members are very positive of the role of the CPI and they would like to see more engagement and direct participation with CPI in various collaborations.

The ECE Department strongly supports the extension of the CPI for another 5-year term.

Sincerely,


Kankar Bhattacharya

October 11, 2022

Charmaine Dean, Vice-President, Research and International

Re: Support of the Waterloo Cybersecurity and Privacy Institute

Dear Professor Dean,

I am writing to you to express my full and strong support for the renewal of the Waterloo Cybersecurity and Privacy Institute (CPI). Cybersecurity and privacy are extremely important research areas, which impact national security, provide substantial business opportunities, and will define each individual's freedoms in modern society. Many of the questions addressed in this research area have direct societal implications related to freedom of information, personal privacy, and anonymity. Cybersecurity and privacy are rightfully identified as key global challenges in UW's current strategic plan. While cybersecurity and privacy are prominent areas in Computer Science, a comprehensive approach must include Math, Engineering, Arts, and Science - which can only be accomplished by an overarching institutional approach.

CPI has been highly successful in facilitating collaboration between faculty members in the David R. Cheriton School of Computer Science's Cryptography Security and Privacy (CrySP) research group and other researchers on campus as well as external partners. Wide-ranging interdisciplinary collaboration is critical to sustain Waterloo's current reputation as a leader in the complex field of cybersecurity and privacy. A concerted effort, such as CPI, is critical to develop world-leading and impactful technologies.

From the perspective of the School, CPI is a tremendously successful undertaking. The institute was instrumental in securing funding for a number of important CS initiatives in recent years, such as

- CRC Tier 1 application (Ian Goldberg) was able to refer to CPI as a key institutional infrastructure commitment in support of the CRC's research area.
- RBC-NSERC Industrial Research Chair (Florian Kerschbaum)
- DND-funded research project on secure and reliable networks (Diogo Barradas, Raouf Boutaba)

along with other projects involving partners such as Rogers and CANARIE. In addition to research endeavors, CPI also plays a role in the educational domain by being a trusted and reliable partner in our ongoing efforts to establish an MMath program in Cybersecurity and Privacy.

Given the prominence and ongoing relevance of the research area, the demonstrated successes of the institute, and the ongoing commitment by all involved parties, there is no doubt in my mind that the Cybersecurity and Privacy Institute will continue to benefit the School of Computer Science, other stakeholders, and the university at large. I very much hope and recommend its renewal.

Sincerely,



Raouf Boutaba, Professor of Director
David R. Cheriton School of Computer Science
University of Waterloo



Letters from Heads of Centres/Institutes

05 July 2022

Dr Charmain Dean
Vice President Research & International
University of Waterloo

Re: Renewal of Cybersecurity and Privacy Institute (CPI) Institute

Dear Charmaine,

I am very pleased to enthusiastically provide this letter of support to accompany the renewal application of Waterloo's Cybersecurity and Privacy Institute (CPI). Cybersecurity is of paramount importance to the future of society at large, especially given the rise of AI in recent years. AI systems are ubiquitous, and it is exactly their widespread use that makes them a target from a security point of view. Further, AI systems today are not designed with security in mind. A consequence of this is that AI systems are particularly vulnerable to security attacks of all kinds. It is a clear that there is an urgent need for intensive research on the topic of security of AI systems, both defense mechanisms and attacks.

Fortunately, the CPI is a world-leading center in security and has played a central role in enhancing Waterloo's strong reputation in all aspects of computer security research and scholarship.

In recent years, CPI has led the way in AI security, with many of its members working closely with members at the AI Institute on security and reliability of AI systems. For the University to continue to maintain its excellence in both security and AI, the renewal of the CPI Institute and its continued strong working relationship with the AI Institute is imperative.

As with AI, Cybersecurity cuts across all industries, with the field growing dynamically by leaps




and bounds in our ever-evolving digital future, regionally, nationally, and internationally. The fundamental need for CPI's efforts is evidenced in the demand from Waterloo AI's corporate partners in sectors as diverse as finance, automotive and supply chain to name a few, that are seeking next generation innovative solutions combining AI and Cybersecurity to deliver responsible, ethical, and trustworthy solutions to humanity.

Building on this strong collaboration and overall success of the CPI Institute over the past several years, as the Co-Director of the Waterloo.AI Institute, it gives me great pleasure in very strongly endorsing the renewal application of the CPI Institute.

Please do not hesitate to reach out to me if you have any additional questions.

Sincerely,



Vijay Ganesh,
Co-Director, Waterloo AI Institute
Associate Professor, University of Waterloo





28/09/2022
Charmaine Dean
Vice-President, Research & International
University of Waterloo
200 University Avenue West
Waterloo, Ontario

Dear Professor Dean,

On behalf of the Institute for Quantum Computing (IQC), it is with great pleasure that I write this letter strongly supporting the renewal of the University of Waterloo's Cybersecurity and Privacy Institute (CPI).

Since its launch in 2018, CPI has been actively tackling the emerging security challenges of our increasingly digital world, a research theme that significantly overlaps with IQC's goals and mission. CPI is an established leader that advances interdisciplinary research in cybersecurity and technology in Canada. They are well recognized by the community through their member's expert commentary which guides public discourse, even in the midst of highly publicized security breaches.

One of IQC's four core research pillars focuses on quantum communication, which directly intersects with CPI's research expertise area of quantum-safe communication. Our common goals have led to fruitful collaborations and advancements in areas including cybersecurity, quantum-safe algorithms for classical computers, quantum cryptography methods, and quantum key distribution research. Additionally, five of IQC's faculty members are also members of CPI (Thomas Jennewein, Debbie Leung, Norbert Lütkenhaus, Michele Mosca, and Jon Yard). It is only through rich collaborations like ours, between cybersecurity experts and quantum experts, that we can ensure that our technology remains safe and secure for decades to come as new quantum technologies are developed and advanced.

The shared research scope and overlap in members between IQC and CPI has also led to a partnership on CryptoWorks21. Founded by Michele Mosca, a member of both IQC and CPI, CryptoWorks21 is a supplementary training program for graduate students to learn next generation quantum cryptography skills, led out of IQC and aligned with CPI. To date, more than one third of CryptoWorks21 participants have been graduate students or postdoctoral fellows from IQC. Additionally, previous CryptoWorks21 participants from IQC are now making their impact in the quantum information and cryptography fields, as professors and start up founders. The partnership between IQC and CPI on CryptoWorks21 advances the training for tomorrow's leaders in quantum-safe cryptography, ensuring that University of Waterloo research remains at the forefront of the second quantum revolution.

As a founding member of the National Cybersecurity Consortium (NCC), CPI has established collaborations with a variety of academic institutions, industry partners, not-for-profit organizations and government organizations across Canada. CPI's involvement with NCC ensures that Waterloo remains a

FROM THE OFFICE OF THE EXECUTIVE DIRECTOR
Institute for Quantum Computing, University of Waterloo
200 University Avenue West, Waterloo, ON, Canada, N2L 3G1
519.888.7610 | iqc@uwaterloo.ca | uwaterloo.ca/iqc



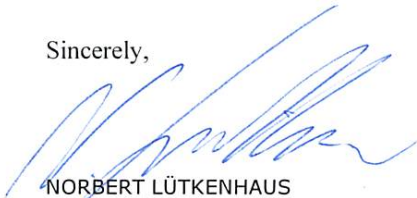
global leader in cybersecurity safety and innovation, and provides IQC members with new networking opportunities.

With the inclusion of humanities faculty members in their research expertise, CPI has also positioned themselves as a leading authority on the ethics, legal questions, and socioeconomic aspects of security and privacy in our increasingly digital world. When new quantum innovations are discovered, it is important to consider the impact of these technologies on society from the beginning of the development process. CPI is a role model for IQC researchers as we consider the implications of our research on society in areas including the protection or loss of personal privacy, the commodification of people as data, and other human-centered challenges.

IQC strongly supports the renewal of CPI, and we are proud of our ongoing partnerships and collaborations. We look forward to continuing and growing our connections as we collaborate on both new and established projects together in the years to come.

It is the belief of myself personally, and on behalf of IQC, that the strong and renewed presence of the Cybersecurity and Privacy Institute will continue to advance the reputation of Waterloo's cutting-edge, quantum-safe cryptography research within the global research community.

Sincerely,



NORBERT LÜTKENHAUS
EXECUTIVE DIRECTOR
INSTITUTE FOR QUANTUM COMPUTING

September 19, 2022

Charmaine Dean, Vice President
Research & International
University of Waterloo

I am writing this letter to express the RoboHub full support to the Cybersecurity and Privacy Institute (CPI) that will be applying for term renewal in the near future. CPI and RoboHub have established a partnership this year, which started with a roundtable session in S2022 that was attended by 20+ researchers in various disciplines from across campus; all of whom found this forum to be very informative. This roundtable forum enabled participants to discuss new interdisciplinary research directions and possible ways to establish new collaborations with colleagues from other departments and faculties across campus.

Also, in discussions with CPI managing director; Mr. Colin Russell, he pointed out that the institute is putting another seed grant call in the fall. In the last call, CPI funded many projects with noticeable research and application merits. Moreover, the National Cybersecurity Consortium (that CPI helped establish) is expected to double the value of the seed grant when CPI researchers apply for the funding in Jan 2023.

The initiatives that CPI is spearheading can help facilities like the RoboHub conduct research in key areas such as robotics systems secure design, privacy concerns, secure networking/information sharing of robot fleets, just to name a few. Through our partnership, we are leveraging world-leading research excellence from both CPI, RoboHub and our partner research labs. This partnership is a growing interdisciplinary venture that aligns well with Waterloo's strategic research priorities.

Therefore, I would like to reiterate my full support to the Cybersecurity and Privacy Institute hoping that the University grants term renewal so that it can continue its successful interdisciplinary research ventures, forge new research partnerships and support academic researchers across campus.

Sincerely,



William W. Melek, PhD, PEng
Professor and Director of RoboHub
Department of Mechanical and Mechatronics Engineering
University of Waterloo
Tel: (519) 888-4567 (ext. 37820)
Fax: (519) 888-6197



July 21, 2022

Dr. Charmaine Dean
Vice President, Research and International
University of Waterloo

Re: Letter of support for the renewal of Waterloo Cybersecurity and Privacy Institute

Dear Dr. Dean:

Please allow me to express my strong support for the University of Waterloo Cybersecurity and Privacy Institute (CPI) renewal. I am currently a Professor of Computer Science, a Tier 1 Canada Research Chair in cybersecurity and founding Director of the Canadian Institute for Cybersecurity (CIC), which I established in the fall of 2016. CIC is a comprehensive multidisciplinary training, research & development, and entrepreneurial Institute with over 100 researchers, students, and staff. I served as the Dean of the Faculty of Computer Science at the University of New Brunswick from 2008 to 2017. I founded the Information Security Centre of Excellence in 2007 and served as its founding Director until 2017. I co-founded the National Cybersecurity Consortium (NCC), which received \$80M in funding from the Federal government in 2022. In 2004, I co-founded the Privacy, Security, Trust (PST) Network in Canada and its annual international conference. I served as the co-Editor-in-Chief of Computational Intelligence: An International Journal for ten years, from 2007 to 2017. I am also a past vice-president of the Canadian Association of Computer Science, served as a CIPS Professional Standards Advisory Council (PSAC) member, and was on the Natural Sciences and Engineering Research Council Committee on Safety and Security. I am a member of Statistics Canada's Advisory Council on Ethics and Modernization of Microdata Access.

According to *Brand Essence* Research, the global cybersecurity market size is projected to reach US\$403 billion by 2027, with a compound annual growth rate of 12.5%. Cybercrime costs organizations US\$2.9 million every minute, and major businesses lose \$25 per minute due to data breaches, according to *RiskIQ* research. In addition, according to a study by IBM, it takes 280 days to find and contain the average cyberattack, while the average cyberattacks costs US\$4.24 million. The average cost of a data breach in Canada was \$6.75 million per incident in the 2021 survey year, higher than the global average.

The University of Waterloo has a long and distinguished history of research excellence in cybersecurity and privacy, with remarkable achievements like pioneering contributions to Elliptic Curve Cryptography and Privacy Enhancing Technologies. It has also been at the forefront of training expert cybersecurity, and privacy researchers in Canada – a significant majority of cybersecurity and privacy faculty members

UNIVERSITY OF NEW BRUNSWICK
540 Windsor Street
Fredericton, NB
Canada E3B 5A3

UNB.CA/CIC



across Canada, are University of Waterloo graduates. However, until 2018, these were individual points of excellence disconnected from one another.

The formation of CPI in 2018 has dramatically changed this situation by helping to coordinate these different activities under a central umbrella, thus helping the University of Waterloo to present a coherent, unified, and effective interface towards other stakeholders in cybersecurity and privacy. An excellent example is how the University of Waterloo contributed to the formation of NCC and its success in securing the major Cybersecurity Innovation Network (CSIN) grant from the federal government. Through CPI, University of Waterloo researchers and staff were able to make a substantial contribution to NCC and its CSIN application process in terms of technical topics and business development for NCC. It is no exaggeration to say that without CPI, the University of Waterloo could not have played such an impactful role in NCC so far. Moreover, CPI will remain a reliable and essential partner for the future success of NCC and its sustainability.

A robust cybersecurity sector is critical for Canada's prosperity and economic stability. Governments recognize the benefits of a connected digital economy and the rising threats from malicious actors seeking to access personal and financial information. I believe the next five years will be a critical period in cybersecurity and privacy innovation and talent development. The University of Waterloo has a critical mass of experts in cybersecurity and privacy across the disciplinary spectrum, ranging from technologists, and mathematicians, to social scientists. The continuation of CPI will be essential for the University of Waterloo to harness the skills and intellect of these experts and channel them towards improving the cybersecurity and privacy research and practice across Canada through NCC, as well as in direct interactions with stakeholders in the industry and other sectors.

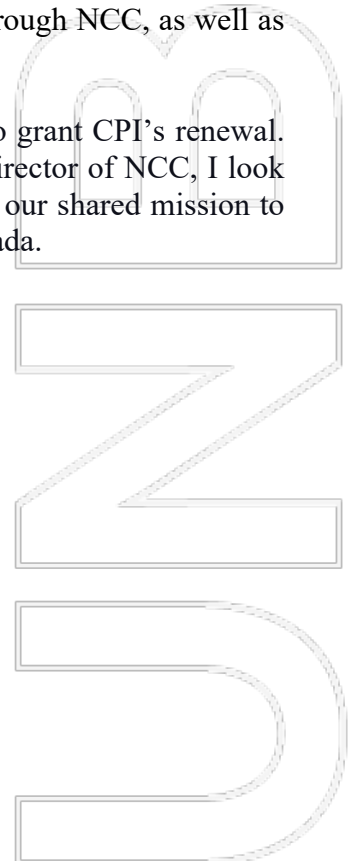
For these reasons, I enthusiastically recommend that the University of Waterloo grant CPI's renewal. As the leader of Canada's oldest cybersecurity institute and as the Managing Director of NCC, I look forward to a continued productive collaboration with CPI and its researchers in our shared mission to deliver technologies and talent to improve cybersecurity and privacy across Canada.

Sincerely,

Ali Ghorbani
Professor and Director

UNIVERSITY OF NEW BRUNSWICK
540 Windsor Street
Fredericton, NB
Canada E3B 5A3

UNB.CA/CIC



Appendix G CPI's Expertise Areas

CYBERSECURITY AND PRIVACY INSTITUTE'S EXPERTISE AREAS



CRYPTOGRAPHY



DATA SCIENCE SECURITY AND PRIVACY



HUMAN AND SOCIETAL ASPECTS OF SECURITY AND PRIVACY



LEGAL AND POLICY ASPECTS OF SECURITY AND PRIVACY



NETWORK SECURITY



OPERATIONAL SECURITY



PRIVACY-ENHANCING TECHNOLOGIES



QUANTUM-SAFE COMMUNICATION



SOFTWARE, HARDWARE, AND SYSTEMS SECURITY

Click Expertise Areas to go directly to section

Integration of CPI expertise areas:



CRYPTOGRAPHY

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of information to view its contents. It provides mathematical and algorithmic tools that are critical for protecting the security of information and communication infrastructures (e.g., the Internet).

Modern cryptography concerns itself with the following four objectives:

- **Confidentiality:** The information cannot be understood by anyone for whom it was unintended
- **Integrity:** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
- **Non-repudiation:** The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information
- **Authentication:** The sender and receiver can confirm each other's identity and the origin/destination of the information

There are many types of cryptography and CPI's faculty specialize in a broad array of cryptographic algorithms, tools, and applications. The table below lists the research focus areas of CPI membership.

SELECTED ILLUSTRATIVE CHALLENGES INCLUDE:

APPLIED CRYPTOGRAPHY

Cryptographic tools for providing confidentiality and security services are now well understood. However, it's still challenging to design and analyze their usage in large-scale applications such as web browsing, messaging, and the Internet of Things. Additional challenges are the efficient and secure implementation of the cryptographic tools, and the design of cryptographic primitives for lightweight environments such as RFID tags.

ADVANCED CRYPTOGRAPHIC PROTOCOLS

Although cryptography is mostly used today to provide basic confidentiality and authentication services, advanced cryptographic techniques can be used to provide a diverse suite of security services including multi-party computation, computing with encrypted data, verifiable computing, and obfuscation. Ongoing research aims to further understand these and related topics in the foundations of cryptography, as well to investigate their emerging applications in cloud computing, blockchain, and privacy-preserving machine learning.

QUANTUM-SAFE CRYPTOGRAPHY

This research field is concerned with the development of cryptographic primitives and protocols that, unlike RSA (an algorithm to encrypt and decrypt general information that is able to withstand brute force attacks in conventional computing) and elliptic curve cryptography, withstand attacks even by large-scale quantum computers. Even though no one can predict with a high degree of certainty when large-scale quantum computers will be built, UWaterloo researchers are already preparing for a possible transition to quantum-safe cryptography.

TABLE 1 CPI RESEARCH TOPICS IN CRYPTOGRAPHY

Research Topic	CPI Experts
<p>Blockchain</p> <p><i>Blockchain is a type of shared database that differs from a typical database in the way that it stores information; blockchains store data in blocks that are then linked together via cryptography.</i></p>	<p>Gordon Agnew Guang Gong Sergey Gorbunov Anwar Hasan</p>
<p>Cryptography for Differential Privacy</p> <p><i>Uses cryptographic primitives to bridge the gap between SDP and LDP. In these solutions, the trusted data curator in SDP is replaced by cryptographic primitives that result in more practical trust assumptions than the SDP model, and better utility than under the LDP model.</i></p>	<p>Xi He</p>
<p>Cryptography for Distributed Systems</p> <p><i>Cryptography to secure a distributed system, which is a computing environment in which various components are spread across multiple computers (or other computing devices) on a network. These devices split up the work, coordinating their efforts to complete the job more efficiently than if a single device had been responsible for the task.</i></p>	<p>Ian Goldberg Sergey Gorbunov</p>
<p>Cryptographic Hardware</p> <p><i>Cryptographic hardware acceleration is the use of hardware to perform cryptographic operations faster than they can be performed in software. Hardware accelerators are designed for computationally intensive software code.</i></p>	<p>Anwar Hasan Mark Aagard</p>
<p>Foundations of Cryptography</p> <p><i>Foundations of cryptography are the paradigms, approaches and techniques used to conceptualize, define, and provide solutions to natural Cryptographic problems.</i></p>	<p>Sergey Gorbunov Mohammad Hajiabadi David McKinnon</p>
<p>Key Establishment</p> <p><i>Key establishment is the process by which two (or more) entities establish a shared secret key. Essentially, two methods are used to establish cryptographic keying material between parties: key agreement and key transport.</i></p>	<p>Ian Goldberg Alfred Menezes Douglas Stebila</p>
<p>Internet Security</p> <p><i>Internet Security consists of a range of security tactics for protecting activities and transactions conducted online over the internet.</i></p>	<p>Ian Goldberg Douglas Stebila</p>
<p>Isogeny-based Cryptography</p> <p><i>Isogeny-based encryption uses the shortest keys of any proposed post-quantum encryption methods, requiring keys roughly the same size as are currently in use.</i></p>	<p>David Jao</p>
<p>Lattice-based Cryptography</p> <p><i>Lattice-based cryptography Is the generic term for constructions of cryptographic primitives that involve lattices, either in the construction itself or in the security proof. Lattice-based constructions are currently important candidates for post-quantum cryptography. Unlike more widely used and known public-key schemes such as the RSA, Diffie-Hellman or elliptic-curve cryptosystems, which could, theoretically, be easily attacked by a quantum computer, some lattice-based constructions appear to be resistant to attack by both classical and quantum computers.</i></p>	<p>Mohammad Hajiabadi Douglas Stebila</p>

Lightweight Cryptography

Lightweight cryptography is an encryption method with a small footprint and/or low computational complexity. It is aimed at expanding the applications of cryptography to constrained devices and the IoT, and its related international standardization and guidelines compilation are currently underway.

Multi-party Computation

Multi-party computation is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptographic tasks, where cryptography assures security and integrity of communication or storage and the adversary is outside the system of participants (an eavesdropper on the sender and receiver), the cryptography in this model protects participants' privacy from each other.

Post-quantum Cryptography

Post-quantum cryptography is cryptographic algorithms (usually public-key algorithms) that are thought to be secure against a cryptanalytic attack by a quantum computer. The problem with currently popular algorithms is that their security relies on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem, or the elliptic-curve discrete logarithm problem. All of these problems can be easily solved on a sufficiently powerful quantum computer running Shor's algorithm.

Privacy-preserving Machine Learning

Privacy-preserving ML is privacy-enhancing techniques concentrated on allowing multiple input parties to collaboratively train ML models without releasing their private data in its original form.

Private Capacity of Quantum Channels

Private capacity of quantum channels is a formula for the capacity of a quantum channel for transmitting private classical information is derived. This is shown to be equal to the capacity of the channel for generating a secret key, and neither capacity is enhanced by forward public classical communication.

Private Information Retrieval

In cryptography, a private information retrieval protocol is a protocol that allows a user to retrieve an item from a server in possession of a database without revealing which item is retrieved.

Pseudorandom Bit Generation

Pseudorandom bit generation is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers, which are important in practice for their speed in number generation and their reproducibility.

Cryptographic applications require the output not to be predictable from earlier outputs, and more elaborate algorithms, which do not inherit the linearity of simpler PRNGs, are needed.

Quantum Cryptanalysis

Quantum cryptanalysis is the study and evaluation of cryptographic algorithms in the presence of a quantum enabled adversary. Quantum computers are expected, within a decade, to be large enough to have an impact on the cryptographic algorithms currently deployed. Hence, the need to study quantum resource requirements to be properly prepared for future quantum-based concerns.

Guang Gong

Ian Goldberg

Mohammad
Hajiabadi

Mohammad
Hajiabadi

David Jao

Alfred Menezes

Michele Mosca

Douglas Stebila

Koray Karabina

Jon Yard

Guang Gong

Xi He

Debbie Leung

Ian Goldberg

Mohammad
Hajiabadi

Guang Gong

Michele Mosca

ACCOMPLISHMENTS

United States National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardization Project: FrodoKEM Submission

Douglas Stebila is a co-author of the **FrodoKEM** protocol, which was one of 69 proposals submitted to the NIST post-quantum cryptography standardization project in 2017. Over the past 4 years, FrodoKEM has advanced through the review process and in 2020 advanced to Round 3 of the process as one of five alternate candidates. In December 2019, the German Federal Office for Information Security began recommending Frodo as one of two algorithms suitable for post-quantum security and continues to recommend Frodo in their annual recommendations.

WAGE: An Authenticated Encryption with a Twist

Designing a lightweight cryptographic primitive requires a comprehensive holistic approach. Guang Gong et. al. have developed **WAGE**, a new lightweight sponge-based authenticated cipher based on the well analyzed Welsch-Gong Permutation (co-developed by Guang Gong and designed for lightweight cryptography). The performance of WAGE balances the tension between hardware efficiency and a good security guarantee. WAGE was a round 2 candidate of the NIST lightweight cryptography competition.

DATA SCIENCE SECURITY AND PRIVACY

The field of data science contains a broad scope, combining multiple fields, such as artificial intelligence, statistics, and data analysis, in an effort to clarify and extract value from data and derive actionable insights. Data science activities centre on preparing data for analysis, including cleansing, aggregating, and manipulating the data to facilitate advanced data analysis. This enables researchers and various analytic applications to be able to discern patterns and statistical significances that lead to informed insights concerning the data's potential utility.

As with all data, privacy and security are of paramount concern when this data is being collected, stored, shared, and erased. The potential for negative consequences should data be compromised is dramatic, including financial, legal, defense-related, compromised democratic and national infrastructure, personal privacy etc.

'Big Data' is fueling the digital economy and companies are amassing vast amounts of personal data. This data can be used to provide improved services in almost all industries, including finance, healthcare, and manufacturing. However, the exploitation of this data also carries the risk of exposing this data to unauthorized or at least unwanted entities, including business partners and end users. Furthermore, when collecting data from many sources, data integrity is not necessarily ensured. Services relying on the data to be correct may be misled by malicious modification to the data. In order to ensure the secure and private use of data, new protection mechanisms need to be developed.

SELECTED ILLUSTRATIVE CHALLENGES INCLUDE:

SECURE AND PRIVATE COLLECTION AND COMBINATION OF DATA SOURCES

Data may be collected by different entities for different business purposes. A typical example is Google collecting data from users clicking on online ads, and Mastercard collecting data from in-store purchases. However, an in-store purchase may have been triggered by an online ad, and only the combination of the data reveals such a connection. Google and Mastercard indeed use private set intersection in order to combine their data sources. Other important examples include private record linkage performed for provincial health care or criminal record checks. Any act of collecting data may raise security and privacy issues. For example, statistics about app use may reveal sensitive information about the user. In order to disguise the data, Apple and Google perturb the data on the client before collection. However, this impacts accuracy so much, such that only very large user bases yield sufficiently accurate statistics.

SECURE AND PRIVATE TRAINING OF MACHINE LEARNING MODELS

Machine learning models may reveal unwanted information about the training data. This may enable attacks on those models, such as membership inference attacks that determine whether a sample was part of the training data set given only the model. Model training may also be disrupted using maliciously crafted poisoning attacks. These attacks may prevent a model from learning the intended behavior or introduce unwanted behavior, called a backdoor. An attacker can trigger the backdoor behavior during inference and cause unintended behavior of the model for the benefit of the attacker. For example, it has been shown that a sticker on a stop sign can cause a model to recognize it as a speeding sign. A special form of training is federated learning where multiple data sources jointly train one machine learning model. However, this carries additional challenges for security and privacy since the process now integrates data collection and training into one process and the defender needs to take care of the entire attack surface.

SECURE AND PRIVATE INFERENCE

Once a machine learning model has been trained, it is used to make predictions over unseen data. However, for privacy concerns, neither the model owner nor the sample owner may want to reveal their data. Hence, privacy-preserving inference protocols are needed. However, even a fully private inference protocol does not prevent a sufficiently powerful adversary from extracting a model using repeated queries, a so-called model extraction attack. This is hard to avoid and the best method for a defender may be to track a model and detect redistribution. Furthermore, an adversary may evade detection by a machine learning model, e.g., used for spam filtering or malware detection, by crafting special inputs. So-called adversarial examples are original samples, e.g., a malware, that have a very small modification, e.g., only a few bytes, but are classified very differently, e.g., a malware as benign software.

TABLE 2 CPI RESEARCH TOPICS IN DATA SCIENCE SECURITY AND PRIVACY

<i>Research Topic</i>	<i>CPI Experts</i>
<p>Reliability of Machine Learning Models</p> <p><i>Building theoretical foundations for defenses and studying their attack resistance against the following: out of distribution data, adversarial examples, random adversaries (random noise models) and semi-random adversaries (mixed random/adversarial corruption models). Developing practical, large-scaled algorithms for real-world AI security problems in computer vision, natural language processing, medical data analysis, etc.</i></p>	<p>Hongyang Zhang</p> <p>Yaoliang Yu</p> <p>Vijay Ganesh</p> <p>Gautam Kamath</p> <p>N. Asokan</p> <p>Ehsan Amjadian</p>
<p>Differential Privacy in Machine Learning Models and Databases</p> <p><i>Developing provably private mechanisms to query databases, visualize data, compute statistics or train machine learning models that improve the privacy vs. accuracy trade-off over existing approaches. Developing and evaluating efficient systems that implement those mechanisms in important applications.</i></p>	<p>Xi He</p> <p>Gautam Kamath</p> <p>Hongyang Zhang</p> <p>N. Asokan</p> <p>Ehsan Amjadian</p>
<p>Privately Linking Data Sources</p> <p><i>Designing cryptographic protocols that can securely and efficiently link data sources and compute functions over their intersection. Developing and evaluating practical deployments for real-world applications in record linkage or fintech.</i></p>	<p>Florian Kerschbaum</p>
<p>Economics of Data Collection and Use</p> <p><i>Understanding the effects of government intervention and policy on the overall societal welfare of industrial data collection and use. Studying mechanisms, such as data markets, to reconcile commercial data use with citizen’s control of private information.</i></p>	<p>Anindya Sen</p>
<p>Mis-/Disinformation</p> <p><i>Studying the spread of mis/disinformation related to collective risks (such as climate change and global pandemics), surveillance, and privacy across a wide variety of national contexts and political regimes. Developing measures and probabilistic models that enable us to better understand when, why, and how mis/disinformation impacts political culture, cognition, deliberation, and identities.</i></p>	<p>John McLevey</p>

ACCOMPLISHMENTS

NSERC/RBC Chair in Data Security

The founding executive director of CPI, Florian Kerschbaum, was able to intensify the relation with Royal Bank of Canada and secure an industrial research chair, the **NSERC-RBC Industrial Research Chair in data security**. The chair's research agenda works in close alignment with RBC's data analytics team and aims to address their privacy challenges. RBC is Canada's largest bank and committed to protecting the privacy of its customers. Florian's team develops solutions that enhance the privacy of RBC's data analytics practice.

CANARIE Joint Security Project

The security of our digital resources, and the infrastructures that support them, are of paramount importance to Canadians, especially Canada's research, education, and innovation communities. The CANARIE Joint Security Project is a community driven approach to addressing the security of these institutions. Raouf Boutaba et. al. developed the **UWaterloo Intrusion Detection System** platform, a data aggregation and analysis hub that ingests more than 1TB of connection data per day from 79 Canadian institutions. It uses both machine learning and graph-based methods, as well as threat feeds, e.g., CanSSOC feeds, to detect threats. The platform provides dashboards and notebooks to visualize and investigate threats and allows sharing of threat intelligence with and between the participating institutions.

HUMAN AND SOCIETAL ASPECTS OF SECURITY AND PRIVACY

The current Digital Age has witnessed an exponential technological development that has enabled individuals to access a wide array of innovative services and goods through the internet and interact with one another through different digital spaces. However, these technological advances have also come with societal costs, such as:

- a loss in individual privacy and the potential for being a victim of cyber-crime
- people being increasingly commodified as data inputs by digital platforms
- massive market power and wealth in the hands of a few large firms
- the emergence of cyber-attacks as significant threats to national security

Faculty members at the University of Waterloo researchers are conducting a wide variety of research that address many of the above issues.

Their research can be broadly classified under the sub-themes of:

- 1) Technology Design
- 2) Behavioral Choices and
- 3) Public Policy.

SELECTED ILLUSTRATIVE CHALLENGES INCLUDE:

TECHNOLOGY DESIGN

The process of how technology is designed, and to what requirements, can incorporate a multitude of influences. Designing technology to improve people's digital experiences, knowledge, and technology practices, with a focus on security, online privacy, and digital literacy is a prime example. Research in this area can investigate the impacts of technology on end user experiences, public perceptions and responses, or policy changes, for example. This research can then, in turn, help inform design choices for future and existing technologies.

BEHAVIOURAL CHOICES

Research in this area covers a broad spectrum of concepts, primarily focusing on the impacts of technology and technology-related variables on the behavioural choices of individuals and/or larger groups. Technology occupies spaces within different paradigms and creates related structures that also have systemic links within different paradigms. For example, surveillance technology impacts how people behave whilst they know they are under scrutiny, whilst the policies that govern surveillance implementation and legality are their own separate but interconnected entity. Research on these relationships can shed light on how technology and technology-related concerns are impacting people's choices and behaviours, leading to greater understanding of how to improve upon these interactions.

PUBLIC POLICY

Public policy encompasses a vast array of different issues related to technology, from surveillance and security studies to ethics and freedom discourses within digital spaces, to governmental and other entity responses to cyberattacks, to name just a few. Public policy research initiatives seek to inform upon any or all of the four stages of public policy formation, namely, agenda setting, formulation, implementation, and evaluation. In essence, research topics and goals seek to expand our understanding of how technology is impacting society, and how existing policy is engaging with these effects, ostensibly with an eye towards positive changes.

TABLE 3 CPI RESEARCH TOPICS IN HUMAN AND SOCIETAL ASPECTS OF SECURITY AND PRIVACY

Research Topic	CPI Experts
<p>Technology Design</p> <p><i>Technology design focuses on improving user experiences, security, and adapting technological designs by increasing the knowledge, data sets, and understanding of technological impacts in a wide array of variables.</i></p>	<p>Phil Boyle</p> <p>Heather Love</p> <p>Marcel Gorman</p> <p>Jennifer Whitson</p> <p>Adam Molnar</p> <p>Urs Hengartner</p> <p>Plinio Morita</p> <p>Leah Zhang-Kennedy</p>
<p>Behavioral Choices</p> <p><i>Behavioral choices research focuses on the impacts of technology and technology-related variables on how individuals and/or larger groups modify their behaviour and choices as a result.</i></p>	<p>Veronica Kitchen</p> <p>John McLevey</p> <p>Alec Cram</p> <p>Maura Grossman</p> <p>Heather Love</p> <p>Marcel Gorman</p> <p>Jennifer Whitson</p> <p>Adam Molnar</p> <p>Urs Hengartner</p> <p>Plinio Morita</p> <p>Leah Zhang-Kennedy</p>
<p>Public Policy</p> <p><i>Public policy research encompasses the study of public policies that govern technology and its implementation, their impacts, and their potential needs for adjustment.</i></p>	<p>Anindya Sen</p> <p>Ian Goldberg</p> <p>Bessma Momani</p> <p>Veronica Kitchen</p> <p>John McLevey</p> <p>Adam Molnar</p> <p>Alec Cram</p>

ACCOMPLISHMENTS

PUPy: A Generalized, Optimistic Context Detection Framework

In modern life, the usage of smart devices like smartphones and laptops that allow for access to information, communication with friends and colleagues and other indispensable services has become ubiquitous. All modern smart devices employ some form of authentication to ensure that access to this confidential data by the wrong person is avoided. This authentication method is usually some form of explicit authentication, which can be detrimental to the user's experience, often leading to users forgoing authentication entirely. Implicit authentication aims to limit the amount of explicit authentications that are necessary for the user, using passive approaches to authenticate the user instead. Context detection frameworks aim to reduce explicit authentications by disabling explicit authentication entirely when appropriate. **PUPy** created by Urs Hengartner and his student Mathew Rafuse, is an open-source context detection framework that can be used for building context-dependent authentication solutions. It provides a large amount of context information through a simple interface, by taking in sensor data and condensing it into three

values - privacy, unfamiliarity, and proximity: Privacy tracks the privacy of the current context; unfamiliarity tracks how many unfamiliar people are around; and proximity estimates the distance between the device and the user.

Paternalistic Surveillance as a Mode of Carceral Expansion

Jennifer Whitson and her student Krystle Shore have been focusing on public health surveillance and its intersection with routine policing practice. Consumer-facing tracking devices are marketed both to police agencies and caregivers of those with Alzheimer's and dementia, allowing both parties to track the movement and habits of their adult wearers. They illustrate how these technologies and services are framed by marketers as a silver bullet solution for aging populations amidst eroded social support networks, but fundamentally operate as coercive and highly commercialized surveillance under a veneer of protection. Vulnerable adults enrolled in the tracking programs by their caregivers become part of a carceral expansion, where data on their movements and habits are shared with first responders and policing agencies. Knowledge of these practices allow the public and regulators to understand the nuances of surveillance and make decisions that balance security and privacy.

LEGAL AND POLICY ASPECTS OF SECURITY AND PRIVACY

Legal and Policy Aspects of Security and Privacy research considers how law and policy shape information environments that relate to cybersecurity and privacy across a range of sectors including health, education, government, consumer, the workplace, and law enforcement. As rapid technological innovations outpace regulatory environments, law and policy research considers how existing law and policy may be insufficient or unfit to facilitate meaningful security and privacy. Researchers under this subtheme also often consider how law and policy are employed as a set of tools to improve the design and delivery of security and privacy.

SELECTED ILLUSTRATIVE CHALLENGES INCLUDE:

PRIVACY LAW AND POLICY REFORM

Privacy and data protection laws are intended to protect the personal information of people as they go about their everyday lives. With the onset of intensely networked digital environments that mediate everyday life, privacy laws often struggle to fulfil their stated purpose. In our era of remote ‘service delivery’, this challenge is further compounded. Research into new technologies—and in diverse settings such as healthcare, education, and the workplace where sensitive personal information is used—is critical to ensure that existing privacy law and policy are adequately understood, evaluated, and reformed where necessary to protect against harms arising from misuse, and to ensure that meaningful regulatory safeguards continue to be advanced for all residents of Canada

DIGITAL HUMAN RIGHTS

As information communication technologies permeate all aspects of social and political life, they disrupt traditional ideas of human rights and governance. New technologies and their application illustrate how pre-existing normative rules no longer neatly map onto our shared digital lives. Questions about the appropriate degree of government and corporate power over individual persons are being recast in our digital age. A key challenge of research in this area is how to adapt the values of constitutionalism to our digital society by assessing the ways that core democratic values such as transparency, accountability, equity, consent, and fairness relate to the technical design and governance of digital environments

GOVERNANCE AND REGULATION BY DESIGN

While regulatory responses routinely include normative rule-based legal and policy approaches to shape particular behavioural outcomes, they also increasingly include technocratic approaches—that is, the purposeful application of technological solutions to facilitate regulatory practices. This form of technological management now encompasses a range of governance sectors—spanning the automation of policing, healthcare, and the workplace, to name but a few. A key challenge noted by researchers in this area relates to ways that technical design of architectures might establish enhanced levels of security and privacy as part of a broader normative rule-based regulatory approach. It also includes a consideration of the impacts of design-related changes as part of the maintenance of social good.

TABLE 4 CPI RESEARCH TOPICS IN LEGAL AND POLICY ASPECTS OF SECURITY AND PRIVACY

Research Topic	CPI Experts
<p>Supervised Machine-Learning for Legal Applications</p> <p><i>The application and evaluation of supervised ML for use in electronic discovery in litigation, in the curation of government records, and for systematic reviews in evidence-based medicine.</i></p>	Maura R. Grossman
<p>Ethical, Legal, and Policy Considerations of Artificial Intelligence and Machine-Learning</p> <p><i>AI systems & ML apply learning techniques to statistics to find patterns in large sets of data and make predictions based on those patterns. Due to the proliferation of AI in high-risk privacy areas, there is an increased focus to design and govern AI to be accountable, equitable, and transparent. This includes studies on how best to serve these goals in legal and policy contexts.</i></p>	Maura R. Grossman Bessma Momani Vijay Ganesh
<p>Understanding the Risks and Regulation of Workplace Surveillance in Canada’s Transition to a Digital Economy</p> <p><i>Employers & employees require guidance navigating and updating transparent equitable policies related to surveillance technologies for employees. These policies must be informed by best practices that protect employee rights, data security, and equitable treatment.</i></p>	Adam Molnar
<p>Responding to Cyber-threats, Cyberattacks, and The Weaponization of Dis/Mis-information</p> <p><i>Focusing on response methods to cyberattacks and the weaponization of dis/misinformation, this research seeks to establish the potential consequences of the (mis)use of information in a digital sphere, and the ways in which these malicious acts can be prevented or mitigated.</i></p>	Bessma Momani Veronica Kitchen
<p>Large-scale Data Governance and Modern Techniques (e.g., Blockchain) for Managing User Consent</p> <p><i>A consent management system allows customers to determine what personal data they are willing to share, which satisfies the lawful requirement for entities to obtain user consent for collecting data, as they are responsible for collecting and managing customer consent. A good consent management process logs and tracks consent collection, and ensures privacy, so that said entities are in compliance with worldwide laws and regulations.</i></p>	Plinio Morita
<p>Maintaining Security, Trust, and Privacy in Health Tech Innovations</p> <p><i>As health data is potentially the most personal and sensitive data for individuals, they must be comfortable sharing this data with a healthcare entity. Healthcare is highly regulated, and health data is a prime target for cybercrime; hence, the very best efforts are required in this area.</i></p>	Adam Molnar Plinio Morita
<p>Surveillance and Privacy in Urban Governance</p> <p><i>Surveillance and privacy in urban governance is helpful to governments, allowing them to gather information and exercise control, which is necessary to fulfill their roles factoring many variables such as increased mobility/anonymity in modern life. Conversely, unchecked surveillance can lead to inequality, discrimination, and repression, undermining a democratic society. Research in this area seeks to promote oversight, accountability, and balance.</i></p>	Phil Boyle

ACCOMPLISHMENTS

Understanding the Risks and Regulation of Workplace Surveillance in Canada’s Digital Economy

In a post-COVID work from home environment protection of individuals' privacy, security, as well as the separation of personal and professional lives from an employer's surveillance is important. Employee monitoring technology is a \$14.5B industry, with significant potential for employer overreach and misuse. This project, helmed by Adam Molnar, is a highly interdisciplinary and inter-sectoral inquiry involving a multi-pronged approach to the issues at hand, combining legal and sociological qualitative inquiry, in conjunction with hardware and software testing. This group provides i) policy recommendations for workplace privacy and cybersecurity both federally and provincially, ii) inform the legal / policy regulation of employee monitoring vendors, iii) software/design related changes that can be a part of these regulatory recommendations, and iv) partnerships with civil society groups such as the British Columbia General Employees' Union (BCGEU) and the Canadian Civil Liberties Association (CCLA). This project is expected to generate resources for the BCGEU that can assist them with negotiating protocol on workplace surveillance and privacy, and with the CCLA on legal analysis and information that they can use on education and awareness on workplace privacy rights for Canadians.

NETWORK SECURITY

Network Security research aims at building secure network infrastructures and communication protocols to protect end users' data, applications, devices, as well as networked assets, from a vast landscape of cyber threats. As businesses increasingly rely on distributed software applications that run across networks, the need for developing holistic solutions that incorporate resource monitoring, access control, threat detection, and attack mitigation capabilities in different operational settings has become a central concern for network administrators.

SELECTED ILLUSTRATIVE CHALLENGES INCLUDE:

SECURE PROTOCOLS FOR DISTRIBUTED SYSTEMS

In today's digitally connected world, a wealth of users' sensitive data like medical records, monetary transactions, or personal information is transmitted through the Internet and efficiently processed by distributed applications hosted in third-party infrastructures, such as the cloud. Ensuring the integrity and confidentiality of data in transit and/or at processing time presents important challenges. First, how can we assess the security of communication protocols? Thus far, network security protocols have been plagued with critical vulnerabilities whose exploitation can prove to be catastrophic. Second, how can we prevent compromised or malicious service providers from breaching users' privacy, e.g., by harvesting the data that users provide to distributed applications? Directions to tackle these issues include the formal security analysis of cryptographic protocols and the design of cryptographic schemes that allow for the outsourcing of computations over encrypted data

DATA-DRIVEN SECURITY AUTOMATION FOR SOFTWARE-DEFINED NETWORKS

Programmable networking devices have enabled the deployment of efficient packet-processing primitives in large-scale and high-speed networks, which can facilitate autonomous diagnosis and localization of network-wide security threats, and execution of countermeasures. However, a challenge lies in dynamically deploying and migrating telemetry and network defence components across the network, and the inability to efficiently collect and process network telemetry data at scale. This can be achieved via intelligent orchestration of software probes, and the development of lightweight and adaptive network monitoring techniques, including in-band network telemetry. The plethora of network data can enable detection and mitigation of threats that can compromise the integrity of systems and data. It is crucial to employ a holistic, multi-faceted approach for threat detection, which capitalizes on different observation points in the network. Furthermore, existing mitigation techniques are often specialized for specific threats, which make them unscalable and impractical. AI techniques are expected to fulfill the promise of automated data-driven detection and mitigation of threats, including zero-day attacks.

SECURITY IN THE ERA OF BLOCKCHAINS

Decentralized cryptocurrencies such as Bitcoin enable digital monetary transactions to be carried out without the presence of a trusted intermediary, whilst concealing the identity of transacting parties. Despite their rising popularity, the mechanisms underpinning decentralized cryptocurrencies lack the ability to interoperate in a secure fashion, or offer the privacy guarantees of in-person cash transactions. These challenges can be addressed by designing novel consensus-based cross-chain communication algorithms, and anonymity-preserving protocols to ensure users' privacy. Moreover, secure naming systems, or public key infrastructures (PKIs), are still quintessential for secure communications, where Blockchain-based PKIs have shown great promise in terms of improved security and resilience compared to traditional centralized PKIs. However, achieving decentralized trust without sacrificing the flexibility and scalability typically found in centralized PKIs, is an open area of research.

MOBILE AND IOT SECURITY

The explosion in the number of "smart" Internet of Things (IoT) devices leveraging various sensors to collect user and environment data is facilitating numerous applications that improve user comfort and convenience, such as automating common household tasks (e.g., smart energy controls), and provide added functionality (e.g., smartphones with fitness tracking capabilities). However, this increases the amount of potentially private information collected by third-party applications, with users having no control on privacy infringement. This challenge can be addressed by: (i) developing IoT traffic filtering mechanisms that provide users the visibility and control over sensor data that is communicated to third-party applications, and (ii) designing differentially private analytics schemes that strike a balance between users' privacy and data utility while analyzing IoT data streams.

TABLE 5 CPI RESEARCH TOPICS IN NETWORK SECURITY

Research Topic	CPI Experts
<p>Secure Protocols for Distributed Systems</p> <p><i>Distributed systems are a network of computing devices that share information and workload to increase efficiency, with the application of cryptographic schemes to secure the data that is transmitted throughout a distributed system, such as a healthcare network.</i></p>	<p>Sergey Gorbunov</p> <p>Douglas Stebila</p> <p>Gordon Agnew</p> <p>Guang Gong</p> <p>Mahesh Tripunitara</p>
<p>Data-driven Security Automation for Software-defined Networks</p> <p><i>Data-driven security automation uses machine learning to analyze big data and improve cybersecurity responses and adaptations. A software-defined network is the ability to abstract the management and administrative capabilities of the technology. With SDN, it's the ability to control the provisioning of network devices, VLANs, firewall rules, etc., and the flow of data.</i></p>	<p>Bernard Wong</p> <p>Raouf Boutaba</p> <p>Diogo Barradas</p>
<p>Security in the Era of Blockchains</p> <p><i>Blockchain technology produces a structure of data with inherent security qualities, based on principles of cryptography, decentralization, and consensus, promoting trust in transactions. It is not infallible however, hence security research to improve blockchain viability is an ongoing initiative.</i></p>	<p>Sergey Gorbunov</p> <p>Raouf Boutaba</p> <p>Guang Gong</p> <p>Sherman Shen</p> <p>Mahesh Tripunitara</p>
<p>Mobile and IoT Security</p> <p><i>Connected devices can be limited in resources in terms of computing power, storage, bandwidth, and energy. Mobile and IoT security applications require adaptive methods for highly diverse contexts utilizing varied resources and conceivably dynamic environments.</i></p>	<p>Urs Hengartner</p> <p>Sherman Shen</p> <p>Guang Gong</p>

ACCOMPLISHMENTS

Data-driven Software-Defined Security

Undoubtedly, businesses and financial institutions are constantly under security threats, which not only costs billions of dollars in damage and recovery, it also detrimentally affects their reputation. A botnet-assisted attack is a widely known threat to these organizations. In this project, Raouf Boutaba et. al. aimed to devise an adaptive and robust botnet detection and mitigation system that leverages machine learning (ML). They proposed novel anomaly-based intrusion detection, employing both host- and network-based detection methods. Each method is strong in detecting some of the essential bot behaviors. Hence, the hybrid detection will leverage the strengths of the underlying methods to build an advanced detection system that bots cannot easily evade. The proposed system will adapt the ML models to network dynamics and adversarial activities, utilizing incremental and adversarial learning, respectively. Upon detection of an intrusion, the system will leverage software-defined networking (SDN) to dynamically adapt the monitoring and surveillance of the network and instigate root cause analysis. The system will automatically generate mitigation workflows that will be enforced via SDN, to ensure integrity of network and its data. The proposed project will broaden the scope of botnet detection and mitigation, including protection against zero-day threats. Advances made in collaboration with the industry partner, Royal Bank of Canada, will have a lasting impact on the design principles and practices of cybersecurity for Canadian businesses and financial institutions. Further, the project has generated 10 publications in prestigious conferences, journals, and magazines.

Axelar:

Sergey Gorbunov is a foundational part of the ongoing development of **Axelar**, a spin-out from Prof. Gorbunov's lab. Axelar is a scalable cross-chain communication platform universal overlay network, securely connecting all blockchain ecosystems, applications, assets, and users to deliver Web3 interoperability. Axelar is composed of a decentralized network of validators, secure gateway contracts, uniform translation, routing architecture, and a suite of software development kits (SDKs) and application programming interfaces (APIs) to enable composability between

blockchains. This allows developers to build on the best platform for their use case, while being able to access users, assets, and applications in every other ecosystem. Instead of pairwise cross-chain bridges, they can rely on a network architecture that provides a uniform code base and governance structure. An exceedingly successful commercial entity, Axelar's latest Series B funding round has brought Axelar's valuation to \$1 billion USD.

Decentralizing Trust with Blockchains

This project focuses on building secure decentralized applications, in particular those around blockchains and related technologies. For instance, an early research outcome was Bitforest and Conifer, a blockchain-based PKI that allows for centralized name administration and efficient lookups but enforces security without trusting any authority. This served as a basis for building SURF (Software Update Registration Framework), a secure blockchain-based software/firmware update system for IoT.

Other ongoing research works include:

Elasticoin: a low-volatility cryptocurrency issuance scheme

Themelio: a new blockchain developed to provide endogenous trust to applications that mostly run outside the blockchain

Astrape: an anonymous payment channel construction. It has generated 4 publications, a patent (US Patent Application No. 16/270,534. Filed February 07, 2019), and a startup

OPERATIONAL SECURITY

Operational security (OPSEC) are the organizational processes deployed to prevent sensitive information from being compromised and seeks to identify threats and activities that could result in critical data being leaked or revealed to a hostile actor. OPSEC processes are most effective when fully integrated into all planning and operational processes. It includes five steps:

- 1) critical data identification
- 2) threat analysis
- 3) vulnerability analysis
- 4) risk analysis
- 5) integration of appropriate countermeasures

The operational security field is keenly interested in ensuring the integrity of information. Information integrity is important because information/data is relied upon in decision making by individuals, organizations, and society as a whole. Information integrity in turn depends on the integrity of the people, processes, and technologies that create the information/data and the integrity of the environments in which those processes function. The quality of information systems/environments depends on the effectiveness of IT governance practices and information systems controls, including controls designed to ensure the security, availability, confidentiality, privacy, and processing integrity of information.

SELECTED ILLUSTRATIVE CHALLENGES INCLUDE:

Information systems assurance involves review, evaluation, and reporting on the integrity of information systems and the information they produce, focusing on the processes used to develop, operate, change, and control those information systems. Information systems assurance services include diagnostic assessments of the strengths and weaknesses of IT governance, assessments of information systems controls, assessments of compliance with management policies, standards and regulatory requirements, assessments of the effectiveness of information systems development, operation and change, and other assessments designed to provide assurance to a variety of stakeholders about the integrity of information systems and the information they produce.

TABLE 6 CPI RESEARCH TOPICS IN OPERATIONAL SECURITY

Research Topic	CPI Experts
<p>Operational Continuity of Mission-critical Information Systems</p> <p><i>Operational continuity of mission critical information systems focuses on designing and assessing mechanisms to ensure the operational continuity of mission-critical information systems through the use of comprehensive controls and effective incident response strategies.</i></p>	<p>Ian McKillop Efrim Boritz Meng Xu</p>
<p>Professional Practice in External/Internal Auditing</p> <p><i>Professional practice in external/internal auditing involves investigating areas of professional practice in external auditing and internal auditing which rely on the exercise of professional judgment and aims to identify factors affecting judgment processes and systematic determinants of judgment quality, with a particular focus on judgement enhancement through decision aids and decision support systems.</i></p>	<p>Efrim Boritz W.Alec Cram</p>
<p>Information Systems Control Initiatives</p> <p><i>Information systems control initiatives focus on how information systems control initiatives can contribute to improving the performance of organizational processes, including systems development and cybersecurity.</i></p>	<p>W.Alec Cram Ian McKillop Efrim Boritz</p>
<p>Automated Program Analysis/Testing/Verification Tools</p> <p><i>This topic intersects with the area of system and software security, with a focus on delivering high-quality solutions to practical security programs, especially in finding and patching vulnerabilities in critical computer systems.</i></p>	<p>Meng Xu</p>

ACCOMPLISHMENTS

OHT Information Management Plan

Ian McKillop contributed to the development of security and privacy policies for one of Ontario's new Health Teams. This includes leading the data collection component of the research, holding workshops with affected stakeholders, analyzing findings, and generating a report of recommendations for a go-forward plan as Ontario engages in a strategy to promote the exchange of data between data custodians in a manner that complies with legislation and reflects best security practices while enabling seamless patient care.

PRIVACY-ENHANCING TECHNOLOGIES

Privacy-enhancing technologies (PETs) research is aimed at empowering people to individually control who can gain access to personal information about them, what those with access can do with that information, and with whom those with access can share the information. Many companies and governments have assembled massive amounts of data about individuals, or are placing restrictions on what information individuals can access, which acutely threatens people's privacy and calls for the ongoing development of new and stronger PETs.

SELECTED ILLUSTRATIVE CHALLENGES INCLUDE:

PROVABLE PRIVACY GUARANTEES

The confluence of recent advances in science and technology, coupled with the ubiquity of massive amounts of data, has ushered in a new era of data-driven analysis and machine learning (ML). However, these algorithms often operate on sensitive data belonging to individuals and generate outputs that leak information about them, like the AOL search data leak and the Facebook-Cambridge Analytica scandal. As such, data-driven companies and organizations must ensure that algorithms respect the privacy of the individuals who provide their data. Our research focuses on developing practical algorithms and systems that support sensitive data analysis and ML with provable privacy guarantees, including differential privacy (DP), a state-of-the-art privacy standard considered in industry and government agencies. The first design issue in existing DP systems is that their utility and performance crucially depend on the privacy expertise level of the user. The targeted users of these analytical data systems are not privacy experts, but they must choose proper parameters and algorithms for their desired utility goal. Second, these systems support limited data types and analyses. Hence, the design needs to be extended to practical settings where data can be multi-relational, unstructured, or even federated. Last, some systems fail to achieve end-to-end privacy guarantees when integrating DP with other cryptographic techniques. This failure motivates us to consider privacy as a first-class citizen in the system design and explore new optimization opportunities such as systems for data analysis and ML.

CENSORSHIP CIRCUMVENTION

Totalitarian states are known to deploy large-scale surveillance and censorship mechanisms in order to deter citizens from accessing a free and open Internet. Thus, considerable effort has been put in place to develop censorship resistance technologies that enable people living (or travelling) in such countries to evade such internet monitoring and blocking mechanisms. Two challenges faced in this context are that these technologies must be able to a) disguise internet traffic that would otherwise be forbidden by a censor as allowed traffic, and b) minimize the ability for a censor that impersonates legitimate clients to enumerate and block endpoints providing the circumvention service. Approaches to tackle these challenges include the generation of proxy-based circumvention tools that build covert channels over popular applications allowed across a censor's border, the design of proxy distribution schemes that minimize the endpoints that are exposed to censors, and the design of in-network circumvention technologies that disregard the need for proxies.

TABLE 7 CPI RESEARCH TOPICS IN PRIVACY ENHANCING TECHNOLOGIES

Research Topic	CPI Experts
<p>Differential Privacy</p> <p><i>DP is a system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset. If the effect of making an arbitrary single substitution in the database is small enough, the query result cannot be used to infer much about an individual, which provides privacy.</i></p>	<p>Xi He</p> <p>Gautam Kamath</p> <p>Florian Kerschbaum</p>
<p>Censorship Circumvention</p> <p><i>Censorship circumvention is the use of various methods and tools to bypass internet censorship. An arms race has developed between censors and developers of circumvention software, resulting in more sophisticated blocking techniques by censors and the development of harder-to-detect tools by researchers.</i></p>	<p>Diogo Barradas</p> <p>Ian Goldberg</p>
<p>Privacy for Machine Learning</p> <p><i>Some ML applications require private individuals' data, which is uploaded to centralized locations in clear text for ML algorithms to extract patterns, and build models from them. Such applications clearly necessitate ML specific privacy protections.</i></p>	<p>N. Asokan</p> <p>Florian Kerschbaum</p> <p>Sherman Shen</p> <p>Yaoliang Yu</p>
<p>Cryptography</p> <p><i>Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.</i></p>	<p>Gordon Agnew</p> <p>Ian Goldberg</p> <p>Guang Gong</p> <p>Koray Karabina</p>
<p>Social Issues</p> <p><i>As most technology and privacy issues involve human interactions and/or impacts, it is important to study these impacts through a lens that focuses on these variables. This includes examining sociological, psychological, and sociopolitical interactions with technology and privacy concerns.</i></p>	<p>Marcel O'Gorman</p> <p>Plinio Pelegrini Morita</p>
<p>Mobile Privacy</p> <p><i>Mobile privacy refers to the privacy rights of users of mobile devices (smartphones, tablets, smart watches, etc.) that are different from and typically additional to the rights of users of internet-based services in general. Mobile devices often contain GPS info, myriad forms of personal data, microphones, and cameras etc., making their security a crucial necessity for users.</i></p>	<p>Urs Hengartner</p> <p>Plinio Pelegrini Morita</p>

ACCOMPLISHMENTS

Improving the Privacy of Tor Onion Services

Privacy-preserving communications networks allow people to communicate with each other, and to access online information, without automatically revealing personal information such as their Internet addresses. The largest such network is The Onion Router (Tor). Ian Goldberg and his work group have contributed significantly to the Tor platform, including the following:

- **PIR for Onion Services**

Private Information Retrieval for Onion Services is a prototype implementation of Tor with support for asynchronous PIR lookups for onion services. Such private lookups prevent malicious Tor onion service directories from learning the relative popularity of onion services or breaking the unlinkability guarantees of Tor's v3 onion service addresses.

- **ConsenSGX**

ConsenSGX is our work on using trusted execution environments such as Intel SGX to allow Tor clients to fetch only small parts of the Tor network consensus document, without opening them up to epistemic attacks.

- **Website fingerprinting**

Website fingerprinting is a classification attack wherein someone watching a user's local network can determine what websites she is visiting, even if she is using privacy enhancing technologies such as encryption, VPNs, or Tor. We have implementations of old and new website fingerprinting attacks and defenses.

- **ExperimenTor**

ExperimenTor is a toolkit and network emulation-based testbed designed to support Tor research in a manner that promotes realism, safety, and scalability. The testbed consists of a set of tools for configuring, running, and analyzing whole-network experiments with an isolated Tor deployment running in the **ModelNet** network emulation platform. We provide the testbed as a set of VMware images that can be used to run Tor experiments out-of-the-box.

Differential Privacy for Databases

Book published in Foundations and Trends in Databases By: Joseph P. Near and Xi He

Differential privacy is a promising approach to formalizing privacy—that is, for writing down what privacy means as a mathematical equation. This book serves as an overview of the state-of-the-art in techniques for differential privacy. The authors focus in particular on techniques for answering database-style queries, on useful algorithms and their applications, and on systems and tools that implement them. These techniques represent significant progress towards building differentially private database systems. The approaches described in this book have already resulted in useful, deployable systems, and likely pave the way towards increasingly widespread adoption of differential privacy in such systems.

QUANTUM-SAFE COMMUNICATION

Quantum-safe Communication research is focused on designing secure communication and computation technologies that would resist attacks by adversaries with quantum computers. Although large-scale quantum computers that are able to break public key cryptography have not yet been built, it is important to start the transition and security research now since today's devices and communications may need to remain secure for decades to come. Many CPI researchers in this research theme are also members or collaborators with the University of Waterloo's Institute for Quantum Computing.

SELECTED ILLUSTRATIVE CHALLENGES INCLUDE:

QUANTUM KEY DISTRIBUTION

Quantum mechanics can be used to construct secure communication technologies. Quantum key distribution (QKD) enables communicating parties to establish a highly secure cryptographic key using quantum optical communication channels. The grand challenge in QKD is to create systems that can communicate at high speeds over long distances

POST-QUANTUM CRYPTOGRAPHY

Whereas quantum key distribution obtains quantum-resistant security by using quantum systems, post-quantum cryptography aims to build quantum-resistant systems using non-quantum algorithms that can be run on existing digital computers and communication systems. There are a variety of mathematical approaches for building post-quantum cryptography, several of which are currently under consideration for standardization. It will be a major undertaking to transition the existing cryptographic infrastructure to use post-quantum algorithms

QUANTUM ALGORITHMS AND CRYPTANALYSIS

In tandem with the design of quantum-resistant systems, equal focus must be paid to the analysis of the ability of quantum computers to break these systems. Quantum cryptanalysis focuses on developing and analysing quantum algorithms for breaking cryptographic assumptions.

TABLE 8 CPI RESEARCH TOPICS IN QUANTUM SAFE COMMUNICATION

Research Topic	CPI Experts
<p>Quantum Information Theory</p> <p><i>Quantum Information Theory is the mathematical theory of information-processing tasks using quantum mechanical systems, such as storage and transmission of information.</i></p>	<p>Debbie Leung</p> <p>Norbert Lütkenhaus</p> <p>Jon Yard</p>
<p>Quantum Algorithms and Cryptanalysis</p> <p><i>Quantum cryptanalysis focuses on developing and analysing quantum algorithms for breaking cryptographic assumptions.</i></p>	<p>Debbie Leung</p> <p>Michele Mosca</p>
<p>Standardization of Post-quantum Cryptography and QKD</p> <p><i>Standardization of post-quantum cryptography and QKD develop new public-key cryptography standards specifying one or more unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.</i></p>	<p>David Jao</p> <p>Thomas Jennewein</p> <p>Norbert Lütkenhaus</p> <p>Michele Mosca</p> <p>Douglas Stebila</p>
<p>Post-quantum Cryptography</p> <p><i>Post-quantum cryptography, or quantum-resistant cryptography, aims to develop cryptographic systems that are secure against both classical and quantum computers, and can work in conjunction with existing networks and communications protocols.</i></p>	<p>Gordon Agnew</p> <p>Guang Gong</p> <p>Mohammad Hajiabadi</p> <p>Anwar Hasan</p> <p>David Jao</p> <p>Alfred Menezes</p> <p>Michele Mosca</p> <p>Douglas Stebila</p> <p>Koray Karabina</p>
<p>Quantum Key Distribution</p> <p><i>QKD is a secure communication method for exchanging encryption keys only known between shared parties, using properties found in quantum physics to exchange cryptographic keys in a manner that is provable and provides security. QKD enables two parties to create and share a key which is then used to encrypt and decrypt messages; QKD is the method of distributing the key, not the key or the data exchanged.</i></p>	<p>Thomas Jennewein</p> <p>Norbert Lütkenhaus</p>

ACCOMPLISHMENTS

Open Quantum Safe Software Project (openquantumsafe.com)

Douglas Stebila and Michele Mosca co-founded the **Open Quantum Safe** (OQP) project. The goal of the project is to develop open-source software for prototyping and evaluating quantum-resistant cryptography and, as of 2021, it is the largest open-source post-quantum cryptography software project in the world. One of the challenges to deploying reliable quantum-safe cryptography was the lack of a reliable open-source platform to support the development and prototyping of post-quantum cryptography. OQS plays an important role in the evaluation of the algorithms being considered for standardization, one of the most important milestones in the practical deployment of post-quantum cryptography. OQS has integrated its cryptography library, liboqs, into a fork of OpenSSL and OpenSSH, and external groups are using it increasingly; including Microsoft’s Post-Quantum Cryptography VPN, Thales eSecurity, Go Wrapper, and Utimaco’s Hardware Secure Module.

OpenQKDSecurity (<https://www.openqkdnetwork.net/>)

Norbert Lütkenhaus and Michele Mosca developed an open-source platform for the numerical analysis of generic QKD protocols. The security analysis of QKD protocols is quite demanding for new researchers entering the field. The underlying mathematical problem is a convex optimization problem. In the past, most effort has been spent on solving those exactly using symmetries of protocols as basis of parameter reduction. The **OpenQKDSecurity** approach converts the problem into a form that can be solved efficiently for general protocols, including those that don't have symmetry. OpenQKDSecurity serves as a platform for interaction between different research communities (experimentalists, cryptographers, mathematicians) that can work on those aspects that correspond to their respective strengths. The entry threshold for new researchers exploring improved protocols is thus lowered.

Canadian Forum for Digital Infrastructure Resilience Quantum Readiness Working Group Michele Mosca chairs the Canadian Forum for Digital Infrastructure Resilience (CFDIR) **Quantum Readiness Working Group**. The CFDIR is a voluntary, consensus-based, and action-oriented public-private collaboration formed to enhance the resilience of the Canadian critical digital infrastructure, resulting in a trusted digital economy for Canadians and a thriving cyber security industry. Innovation, Science and Economic Development Canada (ISED) established CFDIR in 2020, in part to support Canada's National Strategy for Critical Infrastructure. Under this strategy, ISED is the lead federal department for the Information and Communication Technology critical infrastructure sector. CFDIR brings together key federal partners and industry to improve digital infrastructure resiliency.

SOFTWARE, HARDWARE, AND SYSTEMS SECURITY

Software, Hardware, and Systems Security research is aimed at securing the computing devices and the software that runs on them from external cyberattacks. With computing systems being an essential component of every Canadian's life, especially with millions of devices working from home since 2020, it is increasingly important to secure the hardware and software that they depend on.

SELECTED ILLUSTRATIVE CHALLENGES INCLUDE:

VULNERABILITY DETECTION

Vulnerabilities are bugs introduced into the systems by developers unintentionally. Hence, organizations try their best to detect such bugs before the product is released to the public or have security consultants test their released products. Two challenges that exist in such detection is that it is not easy to come up with patterns that can be used to detect vulnerabilities, and when there are patterns, there are a lot of false positives making the technique unusable. Possible approaches include automatic test case generation, fuzzing, static analysis, and penetration testing

CERTIFYING SECURITY PROPERTIES OF SYSTEMS

System developers need to certify the security of their systems. Security flaws in production can be disastrous. In many application domains (e.g., financial, medical, etc.), regulatory requirements mandate strict certification. Possible approaches include Domain Specific Languages, Type Systems, Software Model Checking, and more general Formal Methods

HARDWARE-ASSISTED SOFTWARE PROTECTION

Purely software techniques to protect software systems often involve a tradeoff between the level of security and the performance overhead imposed by the protection technique. Leveraging hardware assistance can avoid this tradeoff but come at the cost of developing and deploying the requisite hardware assistance and the threat of vulnerabilities that arise from the complexity of modern computing hardware itself. The challenge is to develop hardware/software techniques that can avoid these shortcomings

TABLE 9 CPI RESEARCH TOPICS IN SOFTWARE, HARDWARE AND SYSTEMS SECURITY

Research Topic	CPI Experts
<p>Hardware-Assisted Run-Time Protection</p> <p><i>HW-assisted run-time protection is used to harden computer systems against modern run-time attacks; software defenses offer strong security guarantees, but their usefulness is limited by high performance overhead.</i></p>	N. Asokan Cathy Gebotys Ali Mashtizadeh
<p>Ensuring Security Properties with Custom Type Systems</p> <p><i>Custom type systems are used to detect if there exists any kind of violation of confidentiality or integrity in a program.</i></p>	Arie Gurfinkel Werner Dietl
<p>Memory Safety of Low-Level Code</p> <p><i>Memory safety bugs are often security issues, memory safe languages are more secure.</i></p>	Arie Gurfinkel Mei Nagappan N. Asokan Ali Mashtizadeh Meng Xu
<p>Embedded Systems Security</p> <p><i>An embedded system is a programmable hardware component with a minimal operating system and software. Embedded system security is a strategic approach to protecting software running on embedded systems from attack.</i></p>	Sebastian Fischmeister
<p>Software Security</p> <p><i>Software security describes frameworks, processes, methodologies, and strategies that enhance security and reduce vulnerabilities within software and the environment in which it runs. Approaches to software security are frequently structured around potential malicious cyber-attacks.</i></p>	Chengnian Sun Mei Nagappan Yousra Aafer Meng Xu Raouf Boutaba
<p>Mobile/IoT Security</p> <p><i>Mobile (wireless) security is the protection of smartphones, tablets, laptops, and other portable computing devices, and the networks they connect to. Internet of Things (IoT) security is the safeguards and protections for cloud-connected devices such as home automation, security cameras, and any other technology that connects directly to the cloud.</i></p>	Yousra Aafer Mahesh Tripunitara
<p>Formal Methods in Security</p> <p><i>Formal methods are a specific type of mathematically rigorous techniques for the specification, development, and verification of software and hardware systems, in this case, with a security focus.</i></p>	Mark Aargaard Vijay Ganesh Meng Xu Guang Gong Anwar Hasan

ACCOMPLISHMENTS

Hardware-assisted Runtime Protection

Runtime attacks, which involved attacking a program while it is running by exploiting memory vulnerabilities, are endemic. They have featured in most major attacks in the last three decades. While several protection mechanisms have been proposed and implemented, they involve a trade-off between cost of protection and effectiveness. **In this project** N Asokan et. al. explored how this trade-off can be avoided by making use of hardware assistance. Their

work has been funded by NSERC as well as several major industry players, including Intel and Google, resulting in significant top-tier publications.

Android SmartTVs Vulnerability Discovery via Log-Guided Fuzzing

The recent rise of Smart IoT devices has opened new doors for cyber criminals to achieve damages unique to the ecosystem. SmartTVs, the most widely adopted home-based IoT devices, are no exception. To proactively address the problem, Yousra Aafer et. al. proposed a **systematic evaluation of Android SmartTVs security**. They overcame a number of prominent challenges such as most of the added TV related functionalities are (partially) implemented in the native layer and many security problems only manifest themselves on the physical aspect without causing any misbehaviors inside the OS. They developed a novel dynamic fuzzing approach, which features an on-the-fly log-based input specification derivation and feedback collection.

ACKNOWLEDGEMENTS

WE THANK THE FOLLOWING CPI MEMBERS WHO TOOK THE LEAD IN DRAFTING THE PRECEDING DESCRIPTIONS

<i>CRYPTOGRAPHY</i>	ALFRED MENZES
<i>DATA SCIENCE SECURITY AND PRIVACY</i>	FLORIAN KERSHBAUM
<i>HUMAN AND SOCIETAL ASPECTS OF SECURITY AND PRIVACY</i>	ANINDYA SEN
<i>LEGAL AND POLICY ASPECTS OF SECURITY AND PRIVACY</i>	ADAM MOLNAR
<i>NETWORK SECURITY</i>	RAOUF BOUTABA, DIOGO BARADAS
<i>OPERATIONAL SECURITY</i>	IAN MCKILLOP
<i>PRIVACY-ENHANCING TECHNOLOGIES</i>	IAN GOLDBERG, URS HENGARTNER
<i>QUANTUM-SAFE COMMUNICATION</i>	DOUGLAS STEBILA
<i>SOFTWARE, HARDWARE, AND SYSTEMS SECURITY</i>	MEI NAGAPAN, ARIE GURFINKEL

Final Assessment Report

Master of Catholic Thought (MCT)

March 2022

Executive Summary

External reviewers found that the Master of Catholic Thought (MCT) program delivered by St. Jerome's University (SJU) was in good standing.

*The MCT is a quality program that clearly meets UW standards, goals, and outcomes.
The three core faculty who teach and supervise in the program are highly qualified theologians who are invested in the program and committed to student success.*

A total of 4 recommendations were provided by the reviewers, regarding the development of a position description for the MCT Director, publishing a student handbook, and developing a 3–5-year strategic plan for recruitment, stakeholder engagement, curricular development and faculty complement. In response, the program created a plan outlining the specific actions proposed to address each recommendation as well as a timeline for implementation. The next cyclical review for this program is scheduled for 2025-2026.

Enrollment over the past three years

	Graduate enrollment
2021	7
2020	8
2019	4

*based on Active Student Extract from Quest, September 20, 2021.

Background

In accordance with the University of Waterloo's Institutional Quality Assurance Process (IQAP), this final assessment report provides a synthesis of the external evaluation and the internal response of the Master of Catholic Thought program delivered by St. Jerome's University. A self-study (Volume I, II, III) was submitted to the Associate Vice-President, Graduate Studies and Postdoctoral Affairs on December 12, 2019. The self-study (Volume I) presented the program descriptions and learning outcomes, an analytical assessment of the programs, including the data collected from a student survey, along with the standard data package prepared by the Office of Institutional Analysis & Planning (IAP). The CVs for each faculty member with a key role in the delivery of the program(s) were included in Volume II of the self-study.

From Volume III, two arm's-length external reviewers were selected by the Associate Vice-President, Graduate Studies and Postdoctoral Affairs: Dr. Nicholas Olkovich, Assistant Professor and Marie Anne Blondin Chair in Catholic Theology, St. Mark's College; and Dr. Darren Dias, Associate Professor of Theology, St. Michael's College, University of Toronto.

Reviewers appraised the self-study documentation and conducted a virtual site visit to the University from June 22-25, 2020. An internal reviewer from the University of Waterloo, Dr. Hany Aziz, Professor of Electrical and Computer Engineering, was selected to accompany the external reviewers. The visit included interviews with the Vice-President, Academic & Provost; Associate Vice-President, Graduate Studies and Postdoctoral Affairs; Interim President, St. Jerome's University; Interim Vice-President Academic and Dean (VPAD), St. Jerome's University; Dean of the Faculty of Arts; Interim Faculty of Arts Associate Dean of Graduate Studies; Program Director, as well as faculty members, staff and current graduate students. The Review Team was also able to meet with representatives from the library.

Following the site visit, the external reviewers submitted a report on their findings, with recommendations. Subsequently, the program responded to each recommendation and outlined a plan for implementation of the recommendations. Finally, the Dean responded to the external reviewers' recommendations, and endorsed the plans outlined by the program.

This final assessment report is based on information extracted, in many cases verbatim, from the self-study, the external reviewers' report, the program response and the Dean's response.

Program Characteristics

Students in the Master of Catholic Thought (MCT) must take five required courses:

- CT 601: The Books of the Bible
- CT 602: The History of Catholicism
- CT 603: Foundations of Theology
- CT 604: Catholic Moral Life and Thought
- CT 605: The Prayer of the Church: Spirituality and Liturgy

In addition, students are required to take two elective courses. These can be from the list of courses available at St. Jerome's University or from appropriate graduate-level theology courses offered at another University or University College, including Conrad Grebel University College. Students must obtain a minimum overall average of 75, or B, in all courses.

Students are expected to complete a master's-level research paper, 35-50 pages [8,750-12,500 words] long, and to participate in an on-campus Integrative Seminar for CT 606.

To date, all students in the MCT program are part-time students, with students taking one course each term. Due to the decline, over the last few years, of student interest in the Humanities generally and in Religious Studies and Theology programs in particular, undergraduate students

graduating from their programs do not seem to be looking for degrees in theology programs. This is one reason we have not yet seen any full-time enrollments in the MCT program since the inception of the full-time stream in 2016. Attempts will be made to address the issue of full-time enrollment as part of the MCT recruitment plan to be implemented in 2020.

Summary of Strengths, Challenges and Weaknesses based on Self-Study

Strengths

- quality of theological education;
- student experience; student satisfaction; support of students;
- quality of supervision;
- uniqueness of the program across Canada;
- institutional commitment to the program.

Challenges

- recruitment;
- implementation of the full-time option

Weaknesses

- limited course offerings

Summary of Key Findings from the External Reviewers

The MCT is a quality program that clearly meets UW standards, goals, and outcomes. The three core faculty who teach and supervise in the program are highly qualified theologians who are invested in the program and committed to student success. The program also benefits from collaboration with three additional SJU faculty in English, Religious Studies and Philosophy. It is a very small program but constitutes a vibrant learning community. Current students and alumni speak highly of their experience in the program, citing the quality of teaching, in-class discussion, and research paper supervision. Alumni report deep appreciation for their learning experience.

Program Response to External Reviewers' Recommendations

1. Within the next 12 months, develop a position-description for the MCT Director. Currently the position of MCT Director is an interim arrangement. Before a stable appointment is made, it would be beneficial to describe the roles and responsibilities and expected workload of the MCT Director. This is especially important as the program is entering a potentially new stage in its development.

Program Response

Reflecting on the reviewers' remarks, the Committee believes it is time for the MCT program to strengthen its foundations, in particular at the level of program governance. The MCT program clearly needs a stable appointment of a program Director with the vision and experience needed to champion the program. Without this, it will be very difficult to carry the program through the important work needed to ensure that it can be a thriving program into the future. To bring this about, the SJU VPAD would need to make such an appointment, in accordance with the SJU Full-Time Collective Agreement. SJU leadership would also need to decide on the terms of this employment. The Committee welcomes the VPAD's recent formation of an MCT Committee, believing that an advisory body will help to increase program oversight, distribute the work needed to build up and run the program and to generate energy and support from the SJU community. In addition to terms of reference for the program Director, the Committee believes that terms of work for the Committee itself should be developed. Once we have the right structure in place for the program (in addition to a strategic plan – see recommendation 3), we will be able to move forward from a position of much greater strength. The acting Director and newly formed MCT Committee can assist in the development of a position-description as follows:

- Step 1:** The acting MCT Director, in consultation with the MCT Committee, creates a list of all tasks needed to run the MCT program;
- Step 2:** The VPAD reviews the task list and provides feedback;
- Step 3:** The acting MCT Director, in consultation with the MCT Committee, revises the task list and determines the appropriate division of labour and (as applicable) terms of reference for the MCT Director, the MCT Committee, the Academic Administrative Assistant (Morgan Regehr) and any other faculty and/or staff involved with the program (for instance, the members of the Application Review Committee);
- Step 4:** The VPAD reviews and presents the finalized terms of reference for the program Director and MCT Committee to SJU Academic Committee and/or Senate (as appropriate) for approval.
- Step 5:** As part of the appointment process for the MCT program Director, the VPAD creates a position-description drawing from the information gathered in steps 1 and 2.

Academic Dean's Response

The VPAD supports the work that the MCT Committee has undertaken to develop a position-description for the MCT Director and terms of reference for the MCT

Committee. This work will continue in the 2021-2022 academic year as the position-description and terms of reference are finalized.

Faculty of Arts Dean's Response

No additional comment.

2. In the next 12 months, publish a student handbook, or its equivalent. Students have stated that details about the degree are not clearly communicated to them. A brief handbook outlining dates, policies, course mapping, course offerings outside of SJU, auditing, etc. should be published on the website.

Program Response

The reviewers' recommendation to publish a student handbook (or its equivalent) stems from the perceived need for improved communication between MCT program leadership and students. The MCT Committee agrees that this is a legitimate need, however we consider this to be a somewhat lower priority than recommendations 1 and 3, and have reflected this in the timeline at the end of this document. The acting Director, working with the Academic Administrative Assistant, has already taken some steps to rework the SJU–MCT website to provide clearer information for both current and prospective students, and plans to continue this work over the coming year. Whether we need a published handbook in addition to a clearer presentation of necessary information on our website is an open question. The MCT Committee will need to consider how necessary a handbook would be, and what information should be contained in it. The reviewers did not make specific recommendations here beyond offering a very brief list of items (“dates, policies, course mapping, course offerings outside of SJU, auditing, etc.”). We note also that because the MCT program is a conjoint program offered as part of the University of Waterloo's (UW) Faculty of Arts Graduate Studies, there is an additional level of complexity involved because some of the policies relevant to the program are the purview of UW rather than SJU. The following outlines the process for implementing recommendation #2:

- Step 1:** The acting MCT Director, in part by consulting comparable handbooks for other Masters-level theology programs in Canada, generates a draft list of items for inclusion in either a proposed student handbook or an expanded MCT website;
- Step 2:** The MCT Committee reviews the draft list and offers feedback. In discussion of this draft, the Committee also decides on whether or not the publication of a handbook is necessary, rather than simply updating the website.
- Step 3:** Based on the MCT Committee's determination, the MCT Director proceeds either to draft a handbook or to outline a renewed website;

Step 4: The MCT Committee, the VPAD, and the relevant parties in the UW GSPA review the proposed document/website;

Step 5: The MCT Director works with the Academic Administrative Assistant to publish the handbook on the website or to rework the website to include all necessary additional information.

Academic Dean's Response

The VPAD supports the MCT Committee's work to ensure that current and prospective students are able to access all the relevant information needed to complete the program in the way that is most appropriate to the context and delivery of the MCT program.

Faculty of Arts Dean's Response

No additional comment. I am confident that the MCT director and committee are well positioned to determine whether a comprehensive website or handbook would best serve its students in terms of providing information about the program.

3. Develop a 3-5-year strategic plan focusing on the following key result areas and containing appropriate key result indicators. The focus areas and indicators are simply suggestions based on the review; we recognize that the faculty will have to determine if these are appropriate.

3.1 Recruitment: the development of a recruitment strategy should include a focus on:

- i. web and social media presence;
- ii. relationship with undergraduate feeder schools;
- iii. explore possibilities of formal recognition of the MCT as a qualifying program for the Principals Qualification Program/Supervisory Officer Qualification Program;
- iv. explore possibilities of an agreement with the Diocese of Hamilton;
- v. Catholic School Boards, cohort courses for teachers.

Program Response

The MCT Committee is grateful for the reviewers' suggestions concerning a 3-5 year strategic plan for the program. Prior to the review, the program had already begun to act on some of the items that appear in the reviewers' recommendations. For instance, the VPAD appointed the current acting Director in large part to create and carry forward a growth and recruitment (G&R) plan for the program. The acting Director has been working together with the Academic Administrative Assistant (whom SJU also recently hired and whose portfolio includes assisting the MCT program) on various facets of G&R since his

appointment in Sept 2019 (with whatever time remained after focusing on guiding the program review process). The preliminary G&R plan developed during that time anticipated several of the reviewers' suggestions concerning recruitment, and we have already begun to act on some of these. Nevertheless, we acknowledge that in the years leading up to the review recruitment was neglected due to the "administrative shuffle" happening at SJU between 2017 and 2020. Our VPAD had to be brought in as interim President, and our Associate Dean had to be appointed as interim VPAD. This, along with the fact that a functioning MCT Committee had not yet been formed, created a leadership vacuum for the program. The VPAD has now taken several steps to help rectify this, and we are assured of SJU leadership's continuing support for the program in the coming years as we develop and implement our strategic plan.

The Committee welcomes in particular the reviewers' recommendation to increase our intentional outreach to MCT alumni. Since we received the reviewers' report, we have taken the first steps toward engaging alumni by administering a survey designed to elicit alumni preferences for continuing engagement with the program. We intend to increase the presence of the MCT program at events attended by MCT alumni and by representatives of other key stakeholder groups (see our response to 3.2 below). Moving forward with recruitment remains one of our top priorities, and will be the main work of the acting director for the rest of the 2020-2021 academic year once the program review is complete.

We would like to comment on some of the details of the reviewers' other suggestions concerning recruitment. We begin by noting that we have already begun to take steps toward 3.1.i. by performing an initial assessment of the MCT program's web presence (on the www.sju.ca and www.uwaterloo.ca websites), and revising those sites. There is certainly more to be done in this area, and this recommendation overlaps significantly with the communication issue identified in the program reviewers' recommendation #2. As part of our response to 3.1.i, we intend to hire a web/social media consultant in the coming months to form a strategy to increase the MCT program's visibility online. We also intend to conduct recorded interviews with MCT alumni to give them an opportunity to share their experience with the program, its importance to them, and what their degree has enabled them to do. Segments from these interviews can be used on the MCT website to help potential students understand the value of the program.

We have also begun work on 3.1.iii, 3.1.iv and 3.1.v by holding a preliminary conversation with an MCT alumna who is now serving as the Executive Director of the Institute for Catholic Education, and who previously served as Director of Catechesis for the Diocese of Hamilton for 12 years. This former student has helped us to identify further key contacts within the Diocese and the Catholic School Boards in Southwestern Ontario, and has agreed to assist us in the future as needed. Continuing to build the program's web and social media

presence, and to reach out to the groups identified in 3.1.iii-v will remain a core part of our G&R strategy moving forward. We expect that further conversations with other MCT alumni will help to put us in touch with people in their social and professional networks who can work together to establish education partnerships.

We are less certain about the importance of forming relationships with feeder schools (recommendation 3.1.ii), at least in the short term. We understand “feeder schools” to refer to Ontarian and Canadian undergraduate programs, such as Catholic Studies or Religious Studies, from which students might naturally move on to studies in a related MA program (Reviewer’s Report, p. 8). Our sense is that such students would most likely be looking for a full-time program. Although the MCT program has had a full-time program “on the books” for a few years now, we have up to today never enrolled a full-time student. Furthermore, as the reviewers point out, there are currently a number of issues that need to be addressed before it would be realistic to admit full-time students. Simply put, we do not have the requisite dedicated faculty, and we are not currently able to offer enough courses per year, to enable students to move through the program in less than two years. It is important to recall that the MCT program was originally shaped around a part-time clientele; as a result, the move toward a full-time program will require significant rethinking and restructuring. SJU leadership had begun this work in 2016-2017, when the full-time stream was created, but (as alluded to above) a number of unanticipated events conspired to draw attention away from the MCT program for the next few years.

Furthermore, the program faces a “chicken-and-egg” problem in that increased enrollment will motivate SJU leadership to invest in developing the program further, but a lack of such development will make it more difficult to attract students. The current VPAD at SJU has suggested that we should consider offering more courses only when we have more students in the program. This condition on growing the program in terms of faculty and courses, along with the need to strengthen the program according to its current identity, means that over the next few years we must focus our strategic plan on growing the part-time student body. Once we have a successful and thriving part-time stream in place, we will begin to implement the infrastructure needed to support the full-time stream. And at that point, establishing relationships with feeder schools would become more relevant.

As a final point in relation to recruitment, we note that our current VPAD, Cristina Vanin, who served as Director of the MCT program from its founding up to the end of August 2019, also sits at the table of a few important bodies, including the Partnership in Catholic Education for the Diocese of Hamilton. Our newly appointed President, Peter Meehan, attends a meeting with the Directors of Education and Bishop Crosby that takes place once in the Fall and once in the Spring. Finally, our outgoing (Interim) President and previous VPAD, Scott Kline, has established numerous connections within the Catholic community locally and provincially, and recently accepted a visiting scholar appointment at St. Mark’s in

B.C. to help develop a connection between the theology program there and partners in the B.C. Catholic health care system. As a member of the MCT Committee, Scott will be able to apply his experience and existing connections to help the MCT program to form similar partnerships. Our recruitment strategy should make use of these connections already established by and open to our SJU leaders.

Academic Dean's Response

The VPAD appreciates the work that has been done to date to develop a strategic plan for the MCT program, including a recruitment strategy. Regular conversations have been taking place during the past academic year between SJU senior administration and the Acting MCT Director in support of nurturing the relationships needed to ensure that the value of this program for various Catholic agencies and institutions is clearly communicated and advertised. This strategic work will continue in the upcoming academic year with the intention of implementing some of the recruitment initiatives and directions that have been developed by the MCT Committee.

Faculty of Arts Dean's Response

The Arts Graduate recruitment officer has been able to provide some recruitment support for the MCT, but having a dedicated web/social media consultant for the program would be quite beneficial for attracting an increasing number of students.

I note that the program advertises on its website that it is available full time. If SJU cannot offer it full time at this point, it should probably not state that it does so on the website.

3.2 Stakeholder engagement: Increased intentional engagement with relevant stakeholders:

- i. MCT graduates
- ii. SJU faculty from other divisions
- iii. Diocese of Hamilton
- iv. Catholic School Boards
- v. St Joseph's Healthcare System
- vi. Congregation of the Resurrection and the School Sisters of Notre Dame

Stakeholder engagement can be undertaken in a variety of ways, capitalize on current lecture series and events, specific outreach to the groups above, or an advisory board/group with stakeholder and faculty representation.

Program Response

Increased stakeholder engagement has the potential to strengthen the MCT program in many ways, but the Committee wonders what specific ends the reviewers had in mind in suggesting that this should constitute a major component of the strategic plan. Without a clear sense of the purpose of building up stakeholder engagement, it is somewhat difficult to know how to prioritize this objective in relation to other program needs and priorities.

Speculating somewhat about the possible goals driving this recommendation, we note that half of the stakeholder groups mentioned by the reviewers are also included within the recruitment section (MCT graduates, Diocese of Hamilton, Catholic School Boards). Increased engagement with these partners would dovetail with the goal of boosting recruitment to the program. Increasing engagement with the other three stakeholder groups mentioned might serve a variety of purposes. For instance, the program could attempt to bring in SJU faculty from other divisions (ii) to teach elective courses in the MCT program. This would build on the program's ability to offer students diverse perspectives on the way theology can interact with other disciplines, which is something the reviewers identified as one of the program's strengths. The program could also build connections to the St. Joseph's Healthcare System, perhaps creating experiential learning opportunities and linking these to its bioethics offering (v). On the recruitment side, the MCT program can offer opportunities for theological education to Catholics and non-Catholics working in the Catholic Health Care system. This could appeal to administrators within that system who may be concerned about "mission slippage" at the leadership level given the fact that many are relatively unfamiliar with the Catholic theological tradition. Given the historical connection of SJU to the Congregation of the Resurrection and the School Sisters of Notre Dame (vi), it would not be difficult to find ways to increase engagement with these stakeholders, but the questions remain, to what end would the program undertake this, and with what degree of priority?

In the report, the reviewers briefly suggest some specific ways the program could increase stakeholder engagement. The program could make use of current lecture series at SJU (in particular the lectures in Catholic experience) and other events, presumably by inviting members of the stakeholder groups and thereby building a sense of connection to the program. The MCT Committee hopes to develop a 3-5 minute presentation that could be shared during such lecture events, which have historically been well-attended. The annual Feast held at SJU is another event that draws in many from the Catholic community. These events could feature a short segment in which (for instance) MCT alumni describe their experience with the program and how it has impacted their lives and careers. The reviewers suggest that the program could strike an advisory board/group that would be constituted by a mix of faculty and members of key stakeholder groups. The Committee sees how an advisory group of this sort could provide valuable advice to the program and could help to build and guide initiatives linking the program to other Catholic agencies. For instance,

students could be connected to some of the identified stakeholder groups through service learning / experiential learning opportunities. An ongoing connection with stakeholders could also increase the likelihood of bringing students into the program through connections of the sort the reviewers mention in the recruitment section.

Academic Dean's Response

The MCT Committee is raising some good questions with regard to this recommendation. It is likely that the external reviewers saw an integral relationship between engaging with stakeholders and the development of a recruitment strategy, since those stakeholders could be of significant help in advertising the program and recommending the program to potential students. The VPAD supports the MCT Committee's ongoing work to prioritize the various elements of a robust strategic plan for the MCT program.

Faculty of Arts Dean's Response

I am supportive of this recommendation and note that engagement and recruitment serve a dual purpose. The Master of Public Service degree in ARTS also has an advisory board which has served that program very well in terms of forming connections, keeping the curriculum on the cutting edge, and creating co-op opportunities. An advisory board for the MCT could offer similar benefits.

3.3 Curriculum: curricular assessment and online delivery:

- i. building on the reputation of Waterloo and recent directions in higher education in Ontario and in the theological academy, explore the option of integrating service learning/experiential learning. This could be integrated into core courses, elective courses or the capstone project.
- ii. Since this is a course-based master's program, consider having 1 or 2 other capstones for the program (this may also positively impact recruitment) besides the research paper.
- iii. Develop a long-range course schedule and regular rotation that can assist in student course planning and institutional planning. This will be necessary if the program moves to full-time.
- iv. Explore the possibility of online offerings (in a synchronous format fully online or as a hybrid with students simultaneously online and in-person).

Program Response

In response to 3.3.i, the Committee agrees that there exist excellent opportunities at SJU to incorporate service learning and/or experiential learning into the MCT program. Currently offered to undergraduate students, institution-recognized initiatives include the international Beyond Borders and SJU in Peru programs in addition to three locally-based programs: Beyond U, Encounter KW, and Minka.¹ Each of these initiatives connects in one way or another to social justice concerns that could easily be linked to theology via Catholic teachings on social justice and related elective courses in the MCT program. Furthermore, looking to our neighbours in the Master of Theological Studies (MTS) program at Conrad Grebel College, we note that the leaders of that program have found many ways to connect the academic side of theology with practical and pastoral opportunities in connection with the Mennonite community. The MCT program could benefit from development of similar opportunities within the Catholic community, including practica placements in parish ministries or in health care settings or other social services. A major connection the program could build would be to the Kitchener Working Centre, founded by two SJU alumni. SJU leaders have wanted to establish a greater connection with that organization for some time; the MCT program could help mobilize this and could offer unique benefits to the Working Centre given the greater maturity of our student body.

Recommendation 3.3.ii does not specify what sort of additional capstones might be included in the MCT program in addition to the research paper, but it is not difficult to imagine ways that options could be developed that could make the program more attractive to audiences less interested in the traditional thesis option. The idea of practica noted in the previous paragraph provide one example. This recommendation relates to both 3.1 and 3.2 in that greater connections between the MCT program and relevant partners and stakeholders will result in greater clarity concerning specifically what additional capstones would be most helpful / attractive to potential students.

In response to 3.3.iii, the Committee agrees that the program should develop a long-range course schedule and regular rotation, not only to assist students with planning but also for the same of institutional planning in relation to the program and its needs. We note, however, that for this to be realistic, the prior issue of dedicated faculty and increased student enrollment must be addressed. These points are explored further in our response to 3.4 below.

The MCT program has been wanting to open up possibilities for online offerings (3.3.iv) for some time. SJU has the technological capacity to allow students to participate in courses remotely, through live video chat. At least one instructor has had a student participate in their course in this way. The main steps that are needed to increase capacity for this and

¹ For more information on these programs, visit [Centre for Responsible Citizenship | St. Jerome's University \(sju.ca\)](https://www.sju.ca/centre-for-responsible-citizenship).

make it more of a widespread reality are (1) increased instructor familiarity with the relevant technologies, and (2) advertising the possibility of doing the program remotely. In addition to these steps, the program will also need to clarify whether it will in fact require a residence component for students wanting to take the program remotely (as is stated on the program's website), and what that will involve practically. Currently we do not offer the Spring term introduction to the program, or the concluding seminar that were offered when this residency for remote students was first contemplated; the program will have to decide whether these elements can / should be reinstated.

Academic Dean's Response

The VPAD supports the program's response to this recommendation that various aspects of curricular assessment and delivery be considered. Curriculum development can be incorporated into the broader MCT strategic plan. Furthermore, SJU does have extensive experience with experiential learning at the undergraduate level and could certainly look to make this available to MCT students. It is the case that the remote delivery of courses during the past academic year has meant that both faculty and the University are familiar with what is entailed in this type of course delivery.

Faculty of Arts Dean's Response

I am supportive of this recommendation, particularly the advancement of experiential opportunities for its students. ARTS plans to expand work integrated learning for an increasing number of graduate students, and the MCT is well-placed to offer this additional experience in its program at SJU.

3.4 Faculty complement:

- i. One of the three core faculty members has already retired and other retirements could be imminent. Since faculty research shapes the program, faculty regeneration will be key to shaping the future of the program.
- ii. Given the administrative load of current faculty members and the need to offer more courses each year if the program moves to include a full-time option, we recommend a stable, full-time faculty complement.
- iii. We note a lack of diversity in the faculty (core and otherwise) teaching in the MCT, in terms of both race and gender.

Program Response

SJU senior administrators (VPAD, President) hold the responsibility for hiring new faculty members and developing policies around equitable hiring practices. Therefore, these recommendations seem to fall outside the purview of the MCT leadership (Director and Committee). At the same time, and as also noted above, several current SJU faculty members are able and willing to teach in the program, at least as far as elective courses go. Calls could be put out for elective courses, and the MCT Committee could vet responses. Elective courses make up 28% of the degree program's course requirements (2 of 7 courses). If the program's current elective courses cannot be offered (whether by full-time SJU faculty or by qualified contract academic staff), the program could reconsider its electives in light of the research interests of current SJU faculty who would be willing to teach in the program. We note also a connection between recommendation 3.4 and the first recommendation (concerning the appointment of a stable program Director), which is similarly outside the purview of the program itself. Nevertheless, the Committee agrees with the reviewers that the success of this program will depend on a stable faculty contingent, in order that the MCT program can continue to offer the courses and research paper supervision students need to complete the program. This would require replacements of retiring faculty with permanent positions and temporary replacements of faculty seconded to administrative roles at SJU. This is an urgent matter for the program's currently offered part-time stream and would be all the more important should the program begin to offer its full-time stream.

To date, no faculty members have been hired or appointed specifically to teach in the MCT program. Faculty have instead been drawn from SJU's Religious Studies department, which has fortuitously included a number of trained theologians capable of teaching and supervising in the program and of carrying out related research. There is no guarantee that this situation will continue in the future, since it depends on the ongoing stability of the Religious Studies program itself. The Committee believes that SJU administrators must determine the extent to which they can guarantee that an adequate complement of faculty capable of teaching in the MCT program will continue to exist at SJU. Furthermore, the Committee encourages SJU administrators to consider and respond appropriately to the lack of gender and racial diversity in the current MCT faculty when making future hiring decisions. Such considerations should also play a role in decisions to recruit faculty from other SJU departments and programs to teach in the MCT program.

Academic Dean's Response

In the 2021-2022 academic year, the incoming SJU VPAD will begin the process of developing a new academic plan for St. Jerome's University. Part of that academic planning process will include discussions with regard to the directions that SJU will take with its academic programs. As part of the development of its strategic plan, the MCT program can advocate for the resources needed to grow and sustain the program.

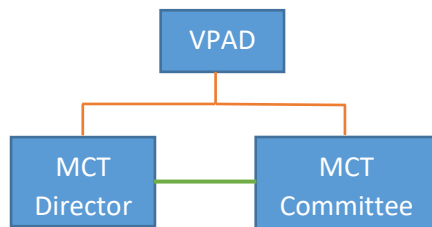
Faculty of Arts Dean's Response

Since faculty complement lies in the province of SJU, not the Faculty of Arts, I have no additional comment here except to note that greater diversity in hiring practices would be well aligned with the objectives of the Arts Faculty as we move forward.

4. The Director of the MCT should submit an annual report on the MCT to the academic body that governs the program whether this is the Senate Council or the Academic Planning Committee.

Program Response

The diagram below depicts the current structure of governance for the MCT program (within SJU), where the orange line represents authority/oversight, and the green line indicates that the Director chairs the MCT Committee:



The MCT program is the only graduate program offered by SJU. It does not normally have representation at Academic Committee, the body at SJU that oversees academic matters for undergraduate programs. Consequently, were the MCT Director to submit an annual report, it would need to go to the VPAD directly, perhaps after having been reviewed by the MCT Committee. It is unclear whether the VPAD would want to receive this sort of report, as the VPAD already receives annual reports from all faculty members, including the MCT Director, containing information related to service (including administrative service). An additional report could be redundant, unless its content was sufficiently distinct (if, for instance, it focused on a review of the program's goals and movement towards those goals, along with descriptive summaries of program activities and challenges). If our VPAD would find this useful, we could include filing such a report among the responsibilities of the program director.

We also note that the reviewers did not elaborate on what the contents of this report would include, or on what its purpose would be. We presume that the goals of such reporting would include ensuring accountability of the program Director and providing an opportunity for feedback and mentorship. The Committee agrees that such accountability

and mentorship by the VPAD could be beneficial, but wonders whether these are not provided for already in the annual report the Director must submit to the VPAD.

The Committee believes that, in making this recommendation, the reviewers were looking for greater accountability for the leadership in the MCT program. We agree that this is a commendable goal. We expect that accountability will increase as a natural result of the regular meeting of the newly formed (as of November 2020) MCT Committee / Advisory Body. Throughout the next 3-5 years, as we develop and implement our strategic plan, and then as we begin to monitor and evaluate our progress in relation to that plan, the MCT Committee plans to meet at least twice per academic term.

Academic Dean's Response

The VPAD supports the MCT Committee's work on developing and implementing a strategic plan that ensures accountability and considers the benefits of regular reporting on the MCT program to the appropriate individuals and bodies at St. Jerome's.

Faculty of Arts Dean's Response

No additional comment.

Recommendations Not Selected for Implementation

N/A

Implementation Plan

	Recommendations	Proposed Actions	Responsibility for Leading and Resourcing (if applicable) the Actions	Timeline for addressing Recommendations
1.	Within the next 12 months, develop a position-description for the MCT Director	<ol style="list-style-type: none"> 1. Generate list of tasks needed to run MCT program 2. Review task list 3. Revise task list and propose a distribution of labour / terms of reference for Program Director and Committee 4. Review and approve terms of reference 5. Appoint a suitable SJU faculty member into a stable (3-year term beginning Fall 2021) position as MCT program director 	<ol style="list-style-type: none"> 1. Acting MCT Director with MCT Committee (and assistance as needed from Academic Admin Coordinator) 2. VPAD 3. Acting MCT Director with MCT Committee 4. VPAD + SJU Academic Committee / SJU Senate 5. VPAD / President 	<ol style="list-style-type: none"> 1. Winter 2021 2. Winter 2021 3. Winter 2021 4. Spring / Fall 2021 5. Spring / Fall 2021
2.	In the next 12 months, publish a student handbook, or its equivalent	<ol style="list-style-type: none"> 1. Propose list of items for inclusion in student handbook (or expanded MCT website) 2. Review proposal and provide feedback 3. Draft handbook/renewed website 4. Review draft 5. Publish handbook / renewed website 	<ol style="list-style-type: none"> 1. Acting MCT Director 2. MCT Committee 3. Acting MCT Director with assistance from Academic Admin Coordinator 4. MCT Committee, VPAD, relevant parties in UW GSPA 5. Academic Admin Coordinator with guidance from Acting MCT Director 	<ol style="list-style-type: none"> 1. Apr-May 2021 2. May-June 2021 3. June-Aug 2021 4. Aug-Oct 2021 5. Oct-Dec 2021

<p>3.</p>	<p>Develop a 3-5-year strategic plan focusing on the following key result areas and containing appropriate key result indicators</p> <p>3.1 Recruitment: the development of a recruitment strategy should include a focus on:</p> <ul style="list-style-type: none"> i. web and social media presence; ii. relationship with undergraduate feeder schools; iii. explore possibilities of formal recognition of the MCT as a qualifying program for the Principals Qualification Program/Supervisory Officer Qualification Program; iv. explore possibilities of an agreement with the Diocese of Hamilton; v. Catholic School Boards, cohort courses for teachers. <p>3.2 Stakeholder engagement: Increased intentional engagement with relevant stakeholders:</p> <ul style="list-style-type: none"> i. MCT graduates ii. SJU faculty from other divisions 	<ul style="list-style-type: none"> 1. Draft a comprehensive strategic plan beginning from the reviewers’ suggested “key result areas” and incorporating previous work by the acting director. 2. Review proposed strategic plan 3. Revise and begin to implement strategic plan 	<ul style="list-style-type: none"> 1. Acting MCT Director and MCT Committee 2. VPAD 3. Acting MCT Director and MCT Committee 	<ul style="list-style-type: none"> 1. Winter-Fall 2021 2. Fall 2021 3. Fall 2021 / Winter 2022
-----------	--	--	---	---

<p>iii. Diocese of Hamilton iv. Catholic School Boards v. St Joseph’s Healthcare System vi. Congregation of the Resurrection and the School Sisters of Notre Dame</p> <p>3.3 Curriculum: curricular assessment and online delivery:</p> <p>i. building on the reputation of Waterloo and recent directions in higher education in Ontario and in the theological academy, explore the option of integrating service learning/experiential learning. This could be integrated into core courses, elective courses or the capstone project.</p> <p>ii. Since this is a course-based master’s program, consider having 1 or 2 other capstones for the program (this may also positively impact recruitment) besides the research paper.</p> <p>iii. Develop a long-range course schedule and regular rotation that can assist in student course planning and institutional</p>			
--	--	--	--

	<p>planning. This will be necessary if the program moves to full-time.</p> <p>iv. Explore the possibility of online offerings (in a synchronous format fully online or as a hybrid with students simultaneously online and in-person).</p> <p>3.4 Faculty complement:</p> <p>i. One of the three core faculty members has already retired and other retirements could be imminent. Since faculty research shapes the program, faculty regeneration will be key to shaping the future of the program.</p> <p>ii. Given the administrative load of current faculty members and the need to offer more courses each year if the program moves to include a full-time option, we recommend a stable, full-time faculty complement.</p> <p>iii. We note a lack of diversity in the faculty (core and otherwise) teaching in the MCT, in terms of both race and gender.</p>			
4.	The Director of the MCT should submit an annual report on the	1. Acting MCT Director meets with current MCT Committee at least	1. Acting Director and MCT Committee	1. Winter 2021 – Spring 2021.


	<p>MCT to the academic body that governs the program</p>	<p>2 times per academic term to discuss the development, implementation, and evaluation of our 3-5 year strategic plan.</p> <p>2. MCT Director continues to meet with MCT Committee 2 times per academic term for this purpose.</p>	<p>2. Director and MCT Committee</p>	<p>2. Fall 2021- Spring 2026</p> <p>A first report was submitted to senior administration in January 2022; this will continue for the upcoming years.</p>
--	--	---	--------------------------------------	---

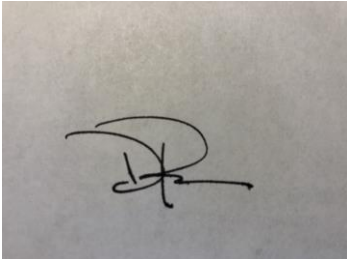
The Department Chair/Director, in consultation with the VPAD and the Dean of Arts shall be responsible for the Implementation Plan.

Date of next program review _____ **2025-2026**
Date

Signatures of Approval


Chair/Director _____ March 22, 2022
Date


AFIW Administrative Dean/Head *(For AFIW programs only)* _____ August 10, 2022
Date



Faculty Dean _____ 17/viii/22
Date
Note: AFIW programs fall under the Faculty of ARTS; however, the Dean does not have fiscal control nor authority over staffing and administration of the program.

Associate Vice-President, Academic _____
(For undergraduate and augmented programs) Date

Jeffrey M. Coakle

March 22, 2022

Associate Vice-President, Graduate Studies and Postdoctoral Affairs
(For graduate and augmented programs)

Date

Final Assessment Report

Doctor of Optometry (OD) and Vision Science (MSc, PhD)

January 2022

Executive Summary

External reviewers found that the Doctor of Optometry (OD) and Vision Science (MSc, PhD) programs delivered by the School of Optometry and Vision Science were in good standing.

“We believe the program is in good standing. Overall students are well trained, they are happy with course material, research in the program is strong, clinical training is excellent, and student outcomes are largely in line with program expectations.”

A total of 4 recommendations were provided by the reviewers, touching on financial resources and the structural deficit carried by the program, a comprehensive review of curriculum, and enabling a stronger focus on research and practice-based scholarship. In response, the program created a plan outlining the specific actions proposed to address each recommendation as well as a timeline for implementation. The next cyclical review for this program is scheduled for 2024-2025.

Student Complement (Total Number of Students Registered in All Levels)

	OD	MSc	PhD
2016-17	364	11	27
2015-16	359	13	27
2014-15	354	18	24

Background

In accordance with the University of Waterloo’s Institutional Quality Assurance Process (IQAP), this final assessment report provides a synthesis of the external evaluation and the internal response of the Doctor of Optometry (OD) and Vision Science (MSc, PhD) programs delivered by the School of Optometry and Vision Science. A self-study (Volume I, II, III) was submitted to the Associate Vice-President, Academic and Associate Vice-President, Graduate Studies and Postdoctoral Affairs on December 14, 2017. The self-study (Volume I) presented the program descriptions and learning outcomes, an analytical assessment of the programs, including the data collected from student surveys, along with the standard data package prepared by the Office of

Institutional Analysis & Planning (IAP). The CVs for each faculty member with a key role in the delivery of the program(s) were included in Volume II of the self-study.

From Volume III, two arm's-length external reviewers were selected by the Associate Vice-President, Academic and Associate Vice-President, Graduate Studies and Postdoctoral Affairs: Dr. Kevin Duffy, Professor in the Department of Psychology and Neuroscience, Dalhousie University, and Dr. Kathryn Murphy, Professor in the Department of Psychology, Neuroscience and Behaviour, McMaster University.

Reviewers appraised the self-study documentation and conducted a site visit to the University on February 13-14, 2018. An internal reviewer from the University of Waterloo, Dr. John Garcia Professor in the School of Public Health and Health Systems, was selected to accompany the external reviewers. The visit included interviews with the Vice-President, Academic & Provost; Associate Vice-President, Academic and Associate Vice-President, Graduate Studies and Postdoctoral Affairs; Dean of Science; Director of the School of Optometry and Vision Science, Faculty members, staff, and groups of current graduate and OD students. The Review Team also had an opportunity to tour the facilities, visit the Clinic and meet with key Clinic personnel, and meet with representatives from the library.

This final assessment report is based on information extracted, in many cases verbatim, from the self-study, the external reviewers' report and the program response.

Program characteristics

Doctor of Optometry (OD): The School of Optometry & Vision Science Doctor of Optometry (OD) is a second entry professional program. The curriculum also reflects expectations and guidance received from external accreditation organizations (Accreditation Council on Optometric Education – ACOE), optometry professional examination organizations (Optometry Examining Board of Canada – OEBC; US National Board Examiners in Optometry – NBEO) and the scope of practice of optometry in North America, generally, and in Canada, specifically. The goals of the program are as follows:

Goal A: The Doctor of Optometry program will provide high quality optometric education which will prepare graduates to provide full-scope optometric services in an ethical and professional manner.

Goal B: The Doctor of Optometry program will provide an optometric foundation on which graduates will continue to build expertise and knowledge.

Goal C: The Doctor of Optometry program will prepare graduates to contribute to the advancement of the optometric profession.

Vision Science (MSc, PhD): The MSc program in Vision Sciences is designed to give students the academic and technical skills to progress in their chosen field in positions requiring graduate training, or to progress to PhD study. The PhD program in Vision Science is designed to give students the academic and technical skills to become independent scientists and researchers.

The primary goal of the graduate programs in Vision Science is to provide a strong research and academic background for graduates. In addition, there is the opportunity for clinicians to enhance their skills and to carry out applied or clinical research. Students are expected to develop self-learning abilities, as well as critical thinking and problem-solving skills. Graduates have secured positions in research, industry, government, healthcare and teaching.

Summary of strengths, challenges and weaknesses based on self-study

Strengths

- The School continues to attract a strong applicant pool from which to select the student cohort.
- Teaching quality of instructors and courses, based on course evaluations, continue to be very good. The faculty have a diverse range of expertise and experience to enhance program teaching and learning.
- Students experience a comprehensive and diverse range of clinical encounters, supported by a vibrant and specialised clinic and external clinical training partners.
- Professional optometric associations at the provincial and national level recognize the important partnership with the School to advance patient access to new and emerging treatments, research, and technology.

Challenges

- The optometry professional program operates on the basis of 12 week terms in the first 3 years, in alignment with the most regular undergraduate programs at the University of Waterloo. This, however, presents a relatively shorter program time compared to other ACOE accredited Schools in the United States and will need creative long-term planning to ensure that it doesn't present a stricture to further development of the curriculum and clinical training.
- Many of sites for the provision of therapeutic externships are located in the United States and represents a suboptimal reliance for the delivery of the program on international partners. A challenge is to develop more Canadian sites that parallel the level of training obtained at the sites in the United States, in accordance with the recommendations of the [Health Professions Regulatory Advisory Council](#).
- To develop budget mechanisms that respect the high cost of clinical training and the motivation to remain contemporary in the fast-moving field of health care (in terms of equipment procurement, development of emerging clinical sub-specialties etc.). The budgetary considerations will also need to address the identified research-intensive

faculty recruitment needs to secure ongoing vibrancy and expansion of the research activities of the School.

- To ensure that the School is ‘training for the profession’s future’ by comprehensively addressing the challenge of providing excellent entry-level training for a variety of jurisdictions, some of which have, or will have, a greater scope of practice than is allowed in Ontario.

Weaknesses

- The processes for ongoing curriculum regeneration need to ensure that there is integration across courses for foundational knowledge, clinical skills, and clinician development and that the curricular architecture is in place to support this. This will enable ongoing and more dynamic curriculum review/adjustments, rather than engaging curriculum review as a periodic process.
- Current assessment of clinical competency is very traditional and needs invigorating to incorporate intentioned formative and summative assessment, reflection on learning to allow the students to develop self-evaluation skills and resourcing of evidence to support their practice. This has learning advantages in that it offers the ability to engage the student more actively in their learning and provides a framework for lifelong learning and professional development. In terms of teaching, a more comprehensive approach to assessment of clinical competency offers mechanisms for efficiently identifying students needing remediation, as well as data for more detailed evaluation of clinical teaching effectiveness. In turn, this will support documentation of teaching activities for the tenure-track clinical professoriate, whose teaching responsibilities are primarily in the provision and supervision of clinical care, and provide sufficient, meaningful data for the tenure process.

Summary of key findings from the external reviewers

“We believe the program is in good standing. Overall students are well trained, they are happy with course material, research in the program is strong, clinical training is excellent, and student outcomes are largely in line with program expectations. A major concern that we detail in our review is the diminished position of the graduate program relative to the OD program, which was evident from the self-study document, and which we believe may partly derive from concerns over research funding, faculty workload, and the recruitment of high-caliber graduate students.

We believe that the program’s priority should be on improving a healthy synergistic relationship between the graduate and OD programs. We recommend that effort be focused on strengthening the graduate program to match the stature of the OD program. This may include renovating research space, providing an environment to facilitate improved success with research funding, and raising the research profile of the graduate program to attract high-quality students.

We further believe that a strategy focused on growth could offer a win-win situation for both programs.”

Program response to external reviewers’ recommendations Recommendations

1. We recommend that the graduate program be allocated financial resources to modernize laboratory space, increase student recruitment success, and build an environment that facilitates high-quality research and improved success with funding.

Response

The School has established a \$50,000 annual seed funding program to support high-quality research initiatives within the School that have potential to attract external funding and graduate students in the near-future. The program provides five \$10,000 grants to collaborative teams each year. The funding can be used to support direct research costs and graduate student support costs. The program began in March 2019 and we will be monitoring research outputs from the program over the next three years.

Writing support workshops and regular writing cafes have been established within the School and are popular. A weekly statistics clinic open to graduate students and faculty has also been established. The aim of these initiatives is to remove barriers to research, publication and grant writing within the School.

We are continuing discussions at the Faculty level to establish a long-term plan for laboratory modernization. Laboratory space is under review with a view to optimising the use of the existing research footprint, to provide collaborative research space and, where necessary, investing in upgrades to meet compliance requirements.

Several larger scale funding initiatives have been undertaken to stimulate research activity. For example, a collaborative initiative with research partners at Hong Kong Polytechnic University has established Centre for Eye and Vision Research in Hong Kong, which received \$200M HK\$ funding over 5 years from the Hong Kong Innovation and Technology Commission to launch operations in the Hong Kong Science Park. The CEVR will pursue broad research areas in the aging eye and visual function, and sight-saving technologies.. A Velux Steifung Foundation grant was applied for and successfully obtained funding for a joint UW/HK Polytechnic University project for a new approach to Age-Related Macular Degeneration treatment that had 6 Optometry and Vision Science faculty members (3 regular and 3 clinical) as named investigators. A CFI application for an imaging centre is being prepared for submission in Fall 2019.

2. We recommend that the OD program commit to a comprehensive review and revision of its teaching curriculum in order to minimize redundancy, improve student engagement, modernize class material, and rejuvenate faculty and student motivation and enthusiasm for the program.

Response

The curriculum committee continues work to implement a modern student-centred curriculum for the contemporary practice of optometry following the standards outlined by the Accreditation Council on Optometric Education ([ACOE](#)). A phased implementation of changes was initiated in Fall 2018. The first phase resulted in streamlining of content in 1st and 2nd year didactic courses by addressing overlaps of material between courses to eliminate redundancies; basic science laboratory courses were rationalized; and two courses were moved from 2nd year to the 1st year (OPTOM 250 Jurisprudence & OPTOM 270 Public Health). The second phase is to review the staging of clinical experience and align clinical teaching assessments with program outcomes.

With this streamlining comes the opportunity to introduce clinical experiences earlier into the curriculum. For example, commencing Fall 2018, 1st year and 2nd year students will interact with patients in the clinic, and will be able to relate their theoretical knowledge to clinical applications.

Implementing clinic earlier within the curriculum will also enable 3rd and 4th year students the clinical proficiency to see a larger number of patients, specifically in our specialty clinics. Other anticipated benefits include shorter patient appointment times and increased student:faculty ratios without compromising the quality of instruction.

The curriculum committee continues to meet with Faculty to garner information and feedback on curriculum changes and is committed to annual curriculum retreat days in which curriculum changes, recommendations and ideas can be discussed.

Investing in technology: The School has benefited from a sizeable donation from FYidoctors to create a state of the art simulation laboratory to enhance student training on diagnostic skills and techniques such as binocular indirect ophthalmoscopy (BIO) and slit lamp biomicroscopy. With increased practice time available and personalized feedback to progress through modules faculty will be able to monitor progression and mastery of the skills and maximize valuable face-to-face lab time for advanced skills development. Increased confidence and efficiency will in turn lead to an enhanced patient care experience, and the more efficient delivery of care in the clinic. The simulation technology is proven in several schools and colleges in the US, and has been received enthusiastically by optometry students as an invaluable learning resource. The BIO

simulators were deployed in 2018, and the sit amp simulators will be deployed for Fall 2020.

Advanced scope of practice: Optometric practice in North America is the most advanced in the world. In states such as Oklahoma, Louisiana, and Kentucky, optometrists are licensed to provide minor surgical procedures as well as laser surgery for refractive correction and glaucoma treatment. A model curriculum developed by an American Optometric Association workgroup has been shared with the curriculum committee to affirm areas already being taught, to identify gaps, and to begin the process of implementing additional education and training opportunities to extend, where needed. In addition, several of our faculty are planning to participate in advanced procedures training courses in Winter/Spring 2019 in order to generate capacity for delivery of educational experience in the area of expanded scope of practice in the OD program, and also to provide a national resource for training Canadian practitioners. Plans for offering the certification have been postponed from Fall 2019 to Spring 2020 due to COVID-related restrictions.

Objective Structured Clinical Examinations (OSCE) are the standard for assessing integrative clinical skills in medical education. The School will seek to develop an OSCE for senior years in the OD program, to assess outcomes and allow the students to prepare for licensing examinations which adopt an OSCE assessment. Funding will be sought to support development of the OSCE with a view to implementation in Winter/Spring 2019 as a formative assessment. Business and curricular development plans will be made for multiple OSCE offerings, with a view to the 4th year OSCE forming a summative assessment. Update: with the aid of a Learning Innovation and Teaching Enhancement (LITE) grant, a faculty team led by Dr. Hrynchak designed and delivered the first OSCE examinations in April 2019 to a group of volunteer students in the final year of the program.

The OSCE assessment is used by the Optometry Examining Board of Canada (OEBC) as part of the entry to practice examination required by regulatory authorities for registration/licensure to practice optometry.

Students were very positive about the interactions with standardized patients and organization of the examination. They felt the examination used realistic scenarios, and helped to ease their anxiety in anticipation for sitting for the OEBC. Scholarship outcomes included an abstract, 1 paper accepted for publication (March 2021), and 1 paper under review.

The development of the **Waterloo Eye Institute** as a national resource for the profession and public fits nicely within the goal to develop the capabilities to deliver an integrated

and coordinated model of eye and vision care. In particular, an ambulatory surgical center will enable a new paradigm of optometry-ophthalmology collaboration and coordination being developed in conjunction with the Waterloo Wellington Local Health Integration Network (LHIN) and area hospitals.

3. We recommend the program commit to an assessment of faculty workload with the aim of implementing efficiencies that will enable a stronger focus on research and practice-based scholarship. We recommend that consideration be given to rationalizing workload while respecting the need to build excellences in both professional and research training programs.

Response

The School is in the process of establishing a working group on faculty workload to ensure that workloads associated with research, teaching, clinical duties and service are distributed appropriately and that research active faculty are provided with appropriate time for grant writing and the execution of their research programs. In addition, graduate supervision and graduate course teaching will be counted as teaching activity within workload assessments with an appropriate time allocation.

Recent faculty retirements have led to workload pressure within the School. Two SACAs (School Advisory Committee on Appointments) have been established and tasked with 1) the hiring of clinical lecturers to address high clinical teaching loads within the School (SACA 1) and, 2) the hiring of two regular tenure track faculty members with internationally recognised research programs or the potential for such programs (SACA 2). This hiring process will directly address workload concerns raised by the review committee and enable an acceleration of clinical innovation, research/scholarship and graduate supervision activity within the School. Hiring of the clinical lecturer was complete with Dr. Julie Shaloub assuming her duties in July 2020. Support from the Dean of Science to initiate SACA 2 was approved by the Provost in July 2020.

4. We recommend that the Director initiate discussions with senior administration about the structural deficit carried by the program, with the goal of formulating a sustainable financial plan that will enable growth of the OD and graduate programs. Such discussions could include a consideration for growth of both OD and graduate programs.

Response

Budget discussions with the Dean of Science identified a significant gap of approximately \$962,000 between historical continuity budget and an allocation based on the WBM (Waterloo Budget Model). Strategic priorities were identified and a number of pathways to investigate were suggested to help develop a sustainability plan.

Some options to explore include:

1. Increasing enrollment
 - a. Satellite campus model – increase number of available seats at remote locations and leverage distance learning and partner infrastructure
 - b. Increase available seats at UW – difficult with existing capacity constraints
 - c. Aggressive recruitment of graduate students (domestic >> international)
 - d. The Advanced Standing Doctor of Optometry Program (ASOPP) is a sustainable plan to integrate up to six (6) qualified, internationally graduated optometrists into the 3rd year of the OD program as the International Optometric Bridging Program winds down.

2. Increasing tuition revenue
 - a. Admit international students to the existing complement of 90 seats in the OD program – premium tuition but likely to be unpopular with the profession given the unique situation as the only English-speaking Canadian School.
 - b. Increase tuition – no indication that the MCU-mandated tuition freeze for 2019/20 will be lifted in 2020/21/ Notwithstanding the foregoing, a strong case can be made that the cost of optometric education is not adequately reflected in current funding levels. Benchmark to average tuition of \$51K at US Schools and Colleges of Optometry – while unlikely to be popular with students, it does reflect the truer cost of education.

3. Increasing non-tuition revenue
 - a. Student technology and innovation fee for additional educational services – clinic consumable, equipment purchase and planned replacement, support for new simulation technology, and assessment models such as OSCE.
 - b. Continuing professional development – certification programs (e.g., advanced procedures), specialty recognition, on-line masters in clinical optometry, continuing education (live and distance learning).
 - c. Clinical services – specialty areas of care are a strength for academic health centers and may provide a significant revenue stream for patient care services such as dry eye/ocular surface disease, myopia control (epidemic amongst Asian population), and vision rehabilitation.
 - d. Waterloo Eye Institute – adding ophthalmological services and partnering with the Waterloo Wellington Local Health Integration Network (LHIN) may open up revenue streams for medical eye care and surgery. Can be initiated in the short term utilizing existing space or in partnership with TLC on-site.

4. Budget requested to support the graduate program and research initiatives are a top priority as evidenced by the consensus process developed through the School Administrative Council (AC). The AC consists of the School Director, Associate

Directors, Clinic Director, graduate officer, undergraduate officer, administrative officer, and 2 faculty members-at-large (1 research/1 clinical). The AC is a deliberative body that represents a cross-section of stakeholders to help inform and advise the School Director.

Additional funding support from the Faculty and University are critical in the short term. For example, GSPA-based budget for scholarships and initiatives will be pursued at every opportunity.

Changes in organization, policy or governance that is necessary to meet the recommendations:

A new governance structure for the School was implemented for Fall 2018. The Admin Council serves as a deliberative body that represents a broad cross section of the School. The Associate Directors and Clinic Director were accorded increased responsibility and budget to lead and manage their respective areas consistent with the strategic plan.

Given that budget and inadequate resourcing is the number one challenge, it will be imperative to conduct a full cost and revenue analysis of the School in anticipation of a request to the government to increase tuition beginning in 2019.

The Waterloo Eye Institute is a strategic imperative for the School that will encompass advantages in patient care for the region, enhanced clinical education, and increased research opportunities. In addition, the Eye Institute will serve as a national resource in support of the public and advancement of the profession as optometry strives to translate cutting edge research into effective, quality patient care outcomes.

Implementation Plan

	Recommendations	Proposed Actions	Responsibility for Leading and Resourcing (if applicable) the Actions	Timeline for addressing Recommendations
1.	<p>We recommend that the graduate program be allocated financial resources to modernize laboratory space, increase student recruitment success, and build an environment that facilitates high-quality research and improved success with funding.</p>	<p><u>Space:</u> Renovation of biomedical laboratory space to meet compliance standards for external auditing bodies.</p> <p><u>Funding:</u> (a) WBRIN-CORD initiative & Hong Kong SAR funding; (b) VELUX funding application; (c) CFI Application; (d) Internal seed funding proposed.</p> <p><u>Research Support Initiatives:</u> Statistics drop-in clinics; Writing workshops.</p>	<p>Prof. Ben Thompson, Associate Director Research 2017-2019</p> <p>Prof. Vivian Choh, Associate Director Research, 2019-present</p>	<p><u>Space:</u> First phase of renovations to biomedical research laboratories due to begin Fall 2019. Delayed because of integration with plans for the WEI and less urgent because of the adverse impact of COVID. Anticipated breaking ground late spring 2022 with completion 12-18 months later.</p> <p><u>Funding:</u> (a) Successfully established WBRIN; Application for HKSAR funding successful, to be announced in Oct 2019; (b) Successfully funded research work at \$270K over 2 yrs; (c) CFI application submission in Fall 2019; updated application proceeding Summer 2022 (d) \$50,000 annual seed-funding to be implemented Mar 2019. Suspended in subsequent years due to COVID.</p> <p><u>Research Support Initiatives:</u> Implemented Jan 2019.</p>



2.	<p>We recommend that the OD program commit to a comprehensive review and revision of its teaching curriculum in order to minimize redundancy, improve student engagement, modernize class material, and rejuvenate faculty and student motivation and enthusiasm for the program.</p>	<p><u>Curriculum:</u> (a) Addressing redundancies in 1st and 2nd year courses; Adjusted course sequencing to allow early clinical exposure in 1st and 2nd years. (b) Staged learning objectives for clinical experience; Corresponding review of assessment strategies to ensure alignment; Review of alignment of preparatory clinical courses and reorganization (if required); (c) Implementation of changes & incorporation of advanced scope of practice training.</p> <p><u>Teaching Innovation:</u> (a) Seek funding support to set up simulation technology for Binocular Indirect Ophthalmoscopy; (b) Develop usage plan for slit lamp and anterior segment techniques, including integration into curriculum, and external training opportunities. Technology likely available at end of Fall 2019/Winter 2020; (c) fully intergrated and an essential resource as patient care services scaled back in response to COVID restrictions. Simulators have been able to help students maintain skills and develop competencies.</p>	<p>Prof. Natalie Hutchings, Associate Director Academics & Student Affairs</p> <p>Dr. Lisa Christian, Associate Director Clinical Education;</p>	<p><u>Curriculum:</u> (a) Completed Fall 2018; (b) In progress; to be completed by Fall 2019; (c) Reorganization and implementation plan by March 2020; (d) adaptation to on-line learning due to COVID with support from faculty was largely successful. In-person clinical labs were supported, and students were able to graduate on time in 2020 and 2021.</p> <p><u>Teaching Innovation:</u> (a) Completed renovation of a suite and installation of BIO simulators Oct 2018 with external support from FYIdoctors. (b) Usage plan in progress anticipated to be complete end of Fall 2019; Implementation dependent on technology availability (proposed at end of Fall 2019/Winter 2020), (c) fully integrated for 2021 including addition of slit lamp biomicroscope simulators.</p>
----	---	--	--	--

		<p><u>Advanced Scope of Practice:</u> (a) Investment of training in faculty in surgical skills; (b) Delivery of training course internally to streamline training curriculum; (c) integrate into OD program and offer training to external optometrists.</p> <p><u>Objective Structured Clinical Examinations (OSCEs)</u> (a) Seek funding for development of OSCE; (b) Develop and implement OSCE as a formative assessment; (c) Develop business and curricular case for multiple OSCE offerings</p> <p><u>Waterloo Eye Institute</u> Development of an ambulatory surgical and diagnostic imaging and reading centre to deliver multi-practitioner coordinated eye and vision care and tele-health. (a) streamlining referrals process; (b) Planning for space and facility;</p>	<p>Dr. Sarah MacIver, Director of Continuing Education;</p> <p>Dr. Patricia Hrynchak, Clinical Professor</p> <p>Dr. Stanley Woo, Director</p>	<p>Advanced Scope of Practice: (a) Faculty training planned for Mar 2019 & August 2019. Complete (b) Planned for August 2020 delayed due to covid restrictions with updated plan for August 2022. (c) Planned for after academic year 2020-2021 with update due to covid for April 2022.</p> <p><u>Objective Structured Clinical Examinations</u> (a) Funding successfully obtained from UW LITE grant to develop OSCE in Fall 2018; (b) OSCE developed and delivered as formative assessment in Winter/Spring 2019; (c) Planning in progress for multiple OSCE deliveries in progress. Delayed because of COVID and shift to on-line activities.</p> <p><u>Waterloo Eye Institute Strategic</u> priority and fundraising for this initiative has begun. (a) Streamlining of referrals in progress – multi-year development (b) Planning for space and facility Spring/Fall 2019. Retained HOK architects with Class C estimate and</p>
--	--	---	---	---

				design submitted in Dec 2021. Consultation with Board of Governors Building and Properties Committee anticipated early 2022.
3.	We recommend the program commit to an assessment of faculty workload with the aim of implementing efficiencies that will enable a stronger focus on research and practice-based scholarship. We recommend that consideration be given to rationalizing workload while respecting the need to build excellences in both professional and research training programs.	<p><u>Faculty workload and working group.</u></p> <p><u>SACA 1</u> hiring committee for clinical lecturers</p> <p><u>SACA 2</u> hiring committee for two regular tenure track faculty members with internationally recognized research programs</p>	Dr. Stanley Woo, Director	<p><u>Faculty Workload and working group</u> Data on workload has been collected; To strike working group in Fall 2019; review WG recommendations and plan for implementation in academic year 2020/2021.</p> <p><u>SACA 1</u> search for clinical lecturers has begun. Anticipated completion in Fall 2019. Completed.</p> <p><u>SACA 2</u> needs assessments has begun; to begin search when funding available for tenure track positions. Completed summer 2021 2 succesful hires – 1 beginning January 2022 and 1 beginning August 2022</p>
4.	We recommend that the Director initiate discussions with senior administration about the structural deficit carried by the program, with the goal of formulating a sustainable financial plan that will enable growth of	<u>Preliminary budget meeting</u>	Dr. Stanley Woo, Director	<u>Preliminary budget meeting</u> completed Spring 2018 & Spring 2019. Agreed upon priorities in alignment with School strategic plan (2018-2023). Annual budget meeting and discussions Feb/March each year.

<p>the OD and graduate programs. Such discussions could include a consideration for growth of both OD and graduate programs.</p>	<p><u>Increasing tuition revenue</u> (a) Increase tuition to reflect elevated cost of clinical education and training in the OD program. Includes addition of a summer term between 2nd and 3rd year necessary to address clinical training and scope of practice in curriculum. Critical to remain competitive with US Schools and Colleges of Optometry and for accreditation. (b) Integration of IOBP students into advanced standing (3rd year of the OD program) (c) BIU funding revenue flow through and updated WGRU accounting.</p>	<p>Dr. Jenna Bright, Director of IOBP/ASOP Dr. Stanley Woo, Director</p>	<p><u>Increasing tuition revenue</u> (a) Proposal to increase to \$48K per year has been socialized with faculty, OD students, and received preliminary approval from the Dean. Seeking university approvals 2019/2020 and government approval 2020, ideally. Update to mid-30K tuition with support from Dean's office. Includes additional term between 2nd and 3rd year Moving forward in Spring 2022 with government relations to gauge timing for submission to MCU. (b) Integration plan initiated Spring 2019; Likely to include no more than 6 students beginning Fall 2021. Transition program beginning summer 2022 with up to 6 students entering 3rd year of the OD program in Fall 2022. (c) Discussions with the Dean have indicated that despite the government indication for a higher level of flow through from BIU to WGRU no</p>
--	---	--	--

		<p><u>Increasing non-tuition revenue</u> (a) Student technology and innovation fee. Fees are presently collected, and may be increased for curriculum enhancement.</p> <p>(b) Continuing Professional Development</p>	<p>Dr. Stanley Woo, Director</p> <p>Dr. Sarah MacIver, Director of CE</p>	<p>additional funding is expected for the School.</p> <p><u>Increasing non-tuition revenue</u> (a) Working with IAP to determine eligibility for fees such as OSCE and simulation equipment. May roll out in coordination with approved tuition fee increase, but ideally sooner (2020). Aligned with policy, but tabled until tuition finalized.</p> <p>(b) Continuing professional development has been established with additional programming planned in spring and fall 2020. E.g. vision therapy symposium and advanced procedures certification course. Certification course for glaucoma offered for Atlantic Provinces in late 2021. Advanced Procedures certification course scheduled for spring 2022.</p>
--	--	--	---	--



Date of next program review _____ 2024-25 _____
Date

Signatures of Approval

20 Jan 2022

Director

Date

AFIW Administrative Dean/Head (For AFIW programs only)

Date

Robert P.
Lemieux

Digitally signed by Robert P.
Lemieux
Date: 2022.01.24 10:58:21 -05'00'

Faculty Dean

Date

Note: AFIW programs fall under the Faculty of ARTS; however, the Dean does not have fiscal control nor authority over staffing and administration of the program.

16 October 2019

Associate Vice-President, Academic
(For undergraduate and augmented programs)

Date

15 October 2019

Associate Vice-President, Graduate Studies and Postdoctoral Affairs

Date

(For graduate and augmented programs)

Two-Year Progress Report

Doctor of Optometry (OD) and Vision Science (MSc, PhD)

June 2022

Background

In accordance with the University of Waterloo's Institutional Quality Assurance Process (IQAP), reviewers appraised the self-study documentation and conducted a site visit to the University on February 13-14, 2018.

Work has been ongoing at the School of Optometry & Vision Science to address the recommendations, and the review has been helpful in aligning and supporting the objectives in the strategic plan and updates.

Enrollment over the past two years

	General	Honours	OD	Grad*
2021-2022 (CURRENT YR)	n/a	n/a	352	30
2020-2021 (LAST YR)	n/a	n/a	354	35

* data source Quest

Progress on Implementation Plan Recommendations

1. We recommend that the graduate program be allocated financial resources to modernize laboratory space, increase student recruitment success, and build an environment that facilitates high-quality research and improved success with funding.

Status: completed

Details

Research funding is included in the operations budget to continue to provide support for activity in alignment with the School's strategic plan. The Associate Director, Research in consultation with the Graduate Studies and Research faculty committee, identify priority areas for funding on an annual basis. In 2022, summer research assistants are the priority

as we resume and ramp up activity post-covid. In parallel, we are implementing promotion strategies to raise awareness about the career pathways provided by a degree in vision science including recruitment for joint OD/MSc degrees.

We are continuing discussions at the Faculty level to establish a long-term plan for laboratory modernization. Laboratory space is under review with a view to optimising the use of the existing research footprint, to provide collaborative research space and, where necessary, investing in upgrades to meet compliance requirements. Biomedical Science space has been designed within the proposed Waterloo Eye Institute. The proposed Canadian Vision Imaging Centre is part of a CFI application (due summer 2022), that includes design plans for research space at the School with funding included in the [Seeing Beyond 2020](#) campaign.

2. We recommend that the OD program commit to a comprehensive review and revision of its teaching curriculum in order to minimize redundancy, improve student engagement, modernize class material, and rejuvenate faculty and student motivation and enthusiasm for the program.

Status: in progress

Details

The curriculum committee continues work to implement a modern student-centred curriculum for the contemporary practice of optometry following the standards outlined by the Accreditation Council on Optometric Education ([ACOE](#)). The second phase is to review the implementation of clinical experience and aligned clinical teaching assessments with program outcomes.

Implementing clinics earlier within the curriculum have enabled 3rd and 4th year students the clinical proficiency to see a larger number of patients, specifically in our specialty clinics. Other anticipated benefits to assess include shorter patient appointment times and increased student to faculty ratios without compromising the quality of instruction.

Regrettably, progress was paused with the onset of the COVID-19 pandemic. Resources were devoted to adapting to on-line delivery of content and assessments. Similarly, re-tooling of clinical labs to minimize in-person contact time was emphasized. Fortunately, the Ministry of Health and Ministry of Colleges and Universities recognized optometry as a health care profession permitted to continue operating in-person clinical laboratories as essential health care workers. Faculty, staff, and students demonstrated incredible

perseverance and resiliency in being able to adapt and graduate on time. Our sister school at Universite de Montreal had their graduating class delayed by several months.

A priority for the curriculum committee this year will be to reflect the increased demands in the depth and breadth of contemporary optometric practice. In particular, advanced procedures to address the growing medical eye care needs of an aging population are evolving in North America. Areas to consider will be the addition of a term between 2nd and 3rd year of the program in order to keep pace with peer accredited programs in the US.

Advanced scope of practice: Optometric practice in North America is the most advanced in the world. In states such as Oklahoma, Louisiana, and Kentucky, optometrists are licensed to provide minor surgical procedures as well as laser surgery for refractive correction and glaucoma treatment. A model curriculum developed by an American Optometric Association workgroup has been shared with the curriculum committee to affirm areas already being taught, to identify gaps, and to begin the process of implementing additional education and training opportunities to extend, where needed. In addition, several of our faculty are certified in advanced procedures and preparing to integrate learning outcomes in the OD program.

The Alberta College of Optometrists endorsed the School of Optometry & Vision Science Advanced Procedures Course certification in 2021. With the mantra of “education before legislation,” the School is recognized as a key partner in expanding scope of practice to help address the growing medical eye care needs of a growing elderly population. Alberta has the highest level for scope of practice in Canada making the School course the anticipated standard for Canada. The plan is for an Advanced Procedures certification course in April 2022 barring public health guidance to the contrary.

Investing in technology: The School has benefited from a sizeable donation from Fyidocors to create a state-of-the-art simulation laboratory to enhance student training on diagnostic skills and techniques. We are anticipating the latest module for gonioscopy in early 2022, a clinical technique important to the diagnosis and management of glaucoma. Simulation technology has been an essential resource to support clinical training during the covid pandemic. Continued investment and innovation in simulation technology is a key priority identified in the School strategic plan.

Objective Structured Clinical Examinations (OSCE) are the standard for assessing integrative clinical skills in medical education. The School will seek to develop an OSCE for senior years in the OD program, to assess outcomes and allow the students to prepare for licensing examinations which adopt an OSCE assessment.

OSCEs were paused at the School in response to the pandemic, and efforts to reduce room occupancy and prolonged contact within 2 m distance. Post-pandemic, we anticipate being able to re-introduce OSCEs to support the curriculum, and our students' preparation to challenge the OEBC, national exams.

The development of the **Waterloo Eye Institute** as a national resource for the profession and public fits neatly within the goal to develop the capabilities to deliver an integrated and coordinated model of eye and vision care. In particular, an ambulatory surgical center will enable a new paradigm of optometry-ophthalmology collaboration and coordination being developed in conjunction with the Waterloo Wellington Local Health Integration Network (LHIN; now KW4 Ontario Health Team), and area hospitals.

3. We recommend the program commit to an assessment of faculty workload with the aim of implementing efficiencies that will enable a stronger focus on research and practice-based scholarship. We recommend that consideration be given to rationalizing workload while respecting the need to build excellences in both professional and research training programs.

Status: in progress

Details

Work was paused due to efforts to adapt teaching and patient care to the covid-19 pandemic restrictions. In 2022, the School will establish a working group on faculty workload to ensure that workloads associated with research, teaching, clinical duties and service are distributed appropriately and that research active faculty are provided with appropriate time for grant writing and the execution of their research programs. In addition, graduate supervision and graduate course teaching will be counted as teaching activity within workload assessments with an appropriate time allocation. The activity will be timely as we map onto processes for the next iteration of the university budget model.

Recent faculty retirements have led to workload pressure within the School. Two SACAs (School Advisory Committee on Appointments) have been established and tasked with 1) the hiring of clinical lecturers to address high clinical teaching loads within the School and, 2) the hiring of two regular tenure track faculty members with internationally recognised research programs or the potential for such programs. Both SACAs were successful resulting in the recruitment of highly qualified faculty – Drs. Julie Shaloub, Clinical Lecturer, William Ngo, Assistant Prof., and Jennifer Hunter, Assoc. Prof. An additional 2 SACAs have been struck in 2022 – 1 for a clinical lecturer in contact lens and myopia control, and another for 2 regular professoriate. The hiring process will directly address

workload concerns raised by the review committee and enable an acceleration of clinical innovation, research/scholarship and graduate supervision activity within the School.

4. We recommend that the Director initiate discussions with senior administration about the structural deficit carried by the program, with the goal of formulating a sustainable financial plan that will enable growth of the OD and graduate programs. Such discussions could include a consideration for growth of both OD and graduate programs.

Status: in progress

Details

Response

Budget discussions with the Dean of Science identified a significant gap of approximately \$962,000 between historical continuity budget and an allocation based on the WBM (Waterloo Budget Model). Strategic priorities were identified and a number of pathways to investigate were suggested to help develop a sustainability plan.

Some options to explore include:

1. Increasing enrollment
 - a. Satellite campus model – increase number of available seats at remote locations and leverage distance learning and partner infrastructure. Deferred until completion of the Waterloo Eye Institute.
 - b. Increase available seats at UW – difficult with existing capacity constraints but anticipating an increase of 6 seats with the implementation of the Waterloo Eye Institute.
 - c. Aggressive recruitment of graduate students (domestic >> international)
 - d. The Advanced Standing Optometry Preparatory Program (ASOPP) is a sustainable plan to integrate up to six (6) qualified, internationally graduated optometrists into the 3rd year of the OD program as the International Optometric Bridging Program winds down. Start date summer 2022.
2. Increasing tuition revenue
 - a. Admit international students to the existing complement of 90 seats in the OD program – premium tuition but likely to be unpopular with the profession given the unique situation as the only Anglophone Canadian School. Recommendation: not feasible.
 - b. Increase tuition – no indication that the MCU-mandated tuition freeze for 2019/20 will be lifted in 2020/21/22. Notwithstanding the foregoing, a strong case can be made that the cost of optometric education is not adequately

reflected in current funding levels. Benchmark to average tuition of \$51K at US Schools and Colleges of Optometry – while unlikely to be popular with students, it does reflect the truer cost of education.

The concept of increased tuition has been socialized with the profession, which recognizes the chronic underfunding of clinical education and training. A proposal to increase tuition has been endorsed by the Dean along with a plan to add an additional term to the program curriculum. The additional term is essential to keep pace with the expanding scope of practice of optometry and to match accredited US competitors who already have had the additional time for many years. Recognition of the cost of delivering clinical education and training is critical with parallels to be made with dentistry being most germane.

3. Increasing non-tuition revenue
 - a. Student technology and innovation fee for additional educational services – clinic consumable, equipment purchase and planned replacement, support for new simulation technology, and assessment models such as OSCE.
 - b. Continuing professional development – certification programs (e.g., advanced procedures), specialty recognition, continuing education (live and distance learning).
 - c. Clinical services – specialty areas of care are a strength for academic health centers and may provide a significant revenue stream for patient care services such as dry eye/ocular surface disease, myopia control (epidemic amongst the Asian population), and vision rehabilitation.
 - d. Waterloo Eye Institute – adding ophthalmological services and partnering with the Waterloo Wellington Local Health Integration Network (LHIN, now KW4 Ontario Health Team) may open up revenue streams for medical eye care and surgery. Can be initiated in the short-term utilizing existing space or in partnership with TLC on-site. Progress still ongoing with the Waterloo Eye Institute.

4. Budget requested to support the graduate program and research initiatives are a top priority as evidenced by the consensus process developed through the School Administrative Council (AC). The AC consists of the School Director, Associate Directors, Clinic Director, graduate officer, undergraduate officer, administrative officer, and 2 faculty members-at-large (1 research/1 clinical). The AC is a deliberative body that represents a cross-section of stakeholders to help inform and advise the School Director.

Additional funding support from the Faculty and University are critical in the short term. For example, GSPA-based budget for scholarships and initiatives will be pursued at every opportunity.

Changes in organization, policy or governance that is necessary to meet the recommendations:

The Waterloo Eye Institute (WEI) is a strategic imperative for the School that will encompass advantages in patient care for the region, enhanced clinical education, and increased research opportunities and impact. In addition, the WEI will serve as a national resource in support of the public and advancement of the profession as optometry strives to translate cutting edge research into effective, quality patient care outcomes.

Explain any circumstances that have altered the original implementation plan

The COVID-19 pandemic has been disruptive to the multiple missions of the School in education, research, and patient care. Faculty have had to adapt courses to on-line delivery, and incorporate safety measures into in-person clinical labs. Similarly, our patient care services have followed directives from Public Health and the College of Optometrists of Ontario to ensure the safe and effective delivery of care and clinical training. Human participant research was significantly curtailed resulting in adverse circumstances for career progress, and also the ability to compete and complete contract industry research (e.g. Centre for Ocular Research and Education, CORE).

The multi-faceted stressors have been recognized throughout the institution. We continue to be amazed by the resiliency and perseverance of our students, staff, and faculty. In spite of the unanticipated hurdles, we continue to move forward together with a clear vision for our collective future.

Address any significant developments or initiatives that have arisen since the program review process, or that were not contemplated during the review

The Waterloo Eye Institute (WEI) emerged as a “Moonshot” initiative as part of our School strategic planning exercise in 2017. From concept to development, we have now reached the threshold for realizing the dream of a centre of excellence in eye and vision care education, research, and patient services.

The Rt. Hon. David Johnston is our Seeing Beyond 2020 campaign chair, and we have close to \$24M raised/pledged towards the \$35M target. Most notably we received \$1M from the Region of Waterloo in December 2021. The WEI will expand regional eye care services AND

catapult forward our research capabilities from fundamental biomedical science through translational efforts to clinical applications and trials.

The review process has complemented our strategic planning, and our most recent update ([May 2021](#)) reflects the incorporation of much of the guidance to strengthen the program. Similarly, the School is well aligned with the University of Waterloo strategic commitment to “lead nationally and globally at the interface of society, health, and technology.”

The World Health Organization published its’ first ever [report on vision](#), and issued a call to action to address a global public health crisis. With an estimated 2 billion people worldwide suffering from vision impairment, it is clear that we have a duty to address the gaps in care with new treatments, innovative delivery models, and new data systems to provide improved outcomes. The WHO report is equally applicable to the Canadian context in individual cost as well as adverse economic impact.

Report on anything else you believe is appropriate to bring to Senate concerning this program

We acknowledge that the timing of reporting has been delayed. However, the intent, planning and implementation has progressed on many fronts in alignment with our strategic plan. We will continue to work diligently to strengthen our School, and reinforce our role as a national resource for the profession and public.

Updated Implementation Plan

	Recommendations	Proposed Actions	Responsibility for Leading and Resourcing (if applicable) the Actions	Timeline for addressing Recommendations
1.	We recommend that the graduate program be allocated financial resources to modernize laboratory space, increase student recruitment success, and build an environment that facilitates high-quality research and improved success with funding.			Complete
2.	We recommend that the OD program commit to a comprehensive review and revision of its teaching curriculum in order to minimize redundancy, improve student engagement, modernize class material, and rejuvenate faculty and student motivation and enthusiasm for the program.	<u>Curriculum:</u> (a) Staged learning objectives for clinical experience; Corresponding review of assessment strategies to ensure alignment; Review of alignment of preparatory clinical courses and reorganization (if required); (b) Implementation of changes & incorporation of advanced scope of practice training.	Prof. Natalie Hutchings, Associate Director Academics & Student Affairs	<u>In progress</u> <u>Curriculum:</u> (a) initiating summer 2022; (b) In progress; to be completed 2024

		<p><u>Teaching Innovation:</u> (a) continued expansion of simulator modules for slit lamp and anterior segment techniques, including integration into curriculum; (b) fully intergrated and an essential resource as patient care services scaled back in response to COVID restrictions. Simulators have been able to help students maintain skills and develop competencies.</p> <p><u>Advanced Scope of Practice:</u> (a) integrate into OD program and offer training to external optometrists.</p> <p><u>Objective Structured Clinical Examinations (OSCEs)</u> (a) Develop business and curricular case for multiple OSCE offerings</p>	<p>Dr. Lisa Christian, Associate Director Clinical Education;</p> <p>Dr. Sarah MacIver, Director of Continuing Education;</p> <p>Dr. C. Lisa Prokopich; Director of Continuing Professional Development</p> <p>Dr. Patricia Hrynchak, Clinical Professor</p>	<p><u>Teaching Innovation:</u> (a) expanded gonioscopy module 2022Q1 for slit lamp biomicroscope simulators; (b) complete</p> <p>Advanced Scope of Practice: (a) integration with curriculum (see above); external training scheduled spring 2022.</p> <p><u>Objective Structured Clinical Examinations</u> (a) Planning in progress for multiple OSCE deliveries in progress. Delayed because</p>
--	--	---	--	--

		<u>Waterloo Eye Institute</u> Development of infrastructure to support multiple missions for research, patient care, and clinical education/training.	Dr. Stanley Woo, Director	of COVID and shift to on-line activities. <u>Waterloo Eye Institute</u> Strategic priority and fundraising for this initiative continues with plans to break ground in 2022.
3.	We recommend the program commit to an assessment of faculty workload with the aim of implementing efficiencies that will enable a stronger focus on research and practice-based scholarship. We recommend that consideration be given to rationalizing workload while respecting the need to build excellences in both professional and research training programs.	(a) establish faculty workgroup to assess workloads associated with research, teaching, clinical duties and service; (b) faculty recruitment in alignment with School strategic plan	Dr. Stanley Woo, Director Prof. Natalie Hutchings, Associate Director Academics & Student Affairs	In-progress (a) initiating workgroup summer 2022; post-pandemic for increased bandwidth; (b) ongoing searches for Clinical Lecturer, and 3 Regular Professoriate
4.	We recommend that the Director initiate discussions with senior administration about the structural deficit carried by the program, with the goal of formulating a sustainable financial plan that will enable growth of the OD and graduate programs. Such discussions could include a consideration for growth of both OD and graduate programs.	Budget Meeting	Dr. Stanley Woo, Director	In-progress Annual budget meeting and discussions Feb/March each year with Dean's Office reviewing agreed upon priorities in alignment with School strategic plan (2018-2023).

		<p>US Schools and Colleges of Optometry and for accreditation.</p> <p><u>Increasing non-tuition revenue</u> (a) Student technology and innovation fee. Fees are presently collected, and may be increased for curriculum enhancement.</p> <p>(b) Continuing Professional Development</p>	<p>Dr. Stanley Woo, Director</p> <p>Dr. Sarah MacIver, Director of Continuing Education;</p> <p>Dr. C. Lisa Prokopich; Director of Continuing Professional Development</p>	<p>gauge timing for submission to MCU.</p> <p><u>Increasing non-tuition revenue</u> (a) Working to set fees such as OSCE, simulation equipment, clerkship support. May roll out in coordination with approved tuition fee increase, but ideally sooner (2023). Aligned with policy.</p> <p>(b) Continuing professional development has been established with additional programming planned in spring and fall 2022. Certification course for glaucoma offered for Atlantic Provinces in late 2021. Advanced Procedures certification course scheduled for spring 2022.</p>
--	--	---	--	--

		<p>(c) Clinical Patient Care Services are an opportunity to deliver exceptional patient care, enhance clinical education and training, as well as drive revenue (especially for specialty services)</p> <p>(d) Waterloo Eye Institute. Major initiative to expand specialty clinical services and provide integrated eye and vision care including surgery (e.g. cataract)</p>	<p>Dr. Andre Stanberry, Clinic Director</p> <p>Dr. Stanley Woo, Director</p> <p>Andrea Carthew, Associate Director, Advancement</p>	<p>(c) Clinical patient care services have undergone a substantive review with periodic fee increases. Additional specialty care services including myopia control and vision therapy expanding but impacted by covid. Addition of UW vision benefit introduced in 2021 and potential for increase in OHIP fees will be beneficial.</p> <p>(d) “Seeing Beyond 2020”. Campaign with Rt. Hon. David Johnston as Honourary Chair coordinated effort with UW Advancement ongoing through 2025.</p>
--	--	--	---	--

The Department Chair/Director, in consultation with the Dean of the Faculty shall be responsible for monitoring the Implementation Plan.

Date of next program review: _____ **2024-25**
Date

Signatures of Approval:



15 February 2022

Director

Date

AFIW Administrative Dean/Head (For AFIW programs only)

Date



August 29, 2022

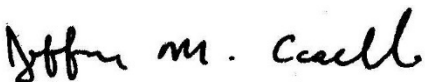
Faculty Dean

Date

Note: AFIW programs fall under the Faculty of ARTS; however, the Dean does not have fiscal control nor authority over staffing and administration of the program.

Associate Vice-President, Academic
(For undergraduate and augmented programs)

Date



16 June 2022

Associate Vice-President, Graduate Studies and Postdoctoral Affairs
(For graduate and augmented programs)

Date

New Program Two-Year Progress Report

Graduate Diploma in Climate Risk Management

August 2021

Background

Climate change is a priority of the 196 national governments that signed the Paris Agreement on Climate Change in 2016. Article 11 of the agreement provides for enhanced capacity building to ensure countries have the necessary skills and knowledge to implement their nationally determined strategies to reduce greenhouse gas emissions and enhance climate resilience of their communities and economies. In Article 12, countries commit to 'enhance climate change education and training' to equip both youth learners and professionals with the competencies and skills required to respond to the challenges of climate change. The province of Ontario has taken a leadership position in addressing climate change. The accelerating transition to a low-carbon and climate resilient economy has created a growing need for specialized education and training across nearly all industry sectors, what some refer to as the emerging "Climate Industry Sector". This program will specifically address the need for this emerging and important sector of work.

A number of international education, training, and workforce needs assessments have concluded that climate change has far-reaching implications for the quantity and location of labour and contributes to the rising demand for increasingly educated and highly skilled employees in several sectors and professions (International Labour Office 2008 - Skills for Green Jobs¹; European Commission 2009 - Climate Change and Employment in the EU-25 to 2030²; UK Government 2010 - Meeting the Low-Carbon Skills Challenge³; International Labour Office 2010 - Climate Change, Its Impacts on Employment and Labour Markets⁴). These workforce needs assessments also concluded that climate policy has remained largely blind to associated training and employment transition needs. In addition to the many new types of climate change positions observed and anticipated to emerge, these assessments also noted a significant need for additional training to familiarize diverse professions and workers with new concepts and

¹ International Labour Office, Skills for Green Jobs, https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_159585.pdf

² European Union. Restructuring Forum: Impact of Climate Change on Employment. <http://www.ec.europa.eu/social/BlobServlet?docId=2863&langId=en>

³ Government of United Kingdom. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/31573/10-849-low-carbon-skills-consultation.pdf

⁴ International Labour Office. Employment and labour market implications of climate change. https://www.ilo.org/gb/GBSessions/WCMS_099711/lang--en/index.htm

practices that will enable them to better participate in a low-carbon economy and engage in climate change risk reduction (termed 'upskilling' of existing competencies).

Therefore, the need to accelerate educational efforts of higher education to equip society to effectively respond to climate change is a recognized priority among international educational institutions. The development of the Graduate Diploma in Climate Risk Management (GDip CRM) will significantly strengthen Ontario's presence in this growing international market.

The approvals process was initiated with statement of interest to Waterloo Quality Assurance (QA) in November 2016. Based on feedback received, the full program brief was developed and submitted to QA on Sept. 14, 2017. Provost approval was received on Nov. 15, 2017. The Faculty of Environment's Graduate Studies Council approved the proposal on Nov. 20, 2017 with Environment Faculty Council approving the proposal via E-vote on Dec. 4, 2017. Approval at Senate Graduate and Research Council was given on Dec. 11, 2017 with the University Senate giving approval in January 2018.

The proposal was reviewed by the Quality Council on Feb. 5, 2018, from which minor clarifications were requested and submitted back on March 29th. The program was approved by the Quality Council April 20, 2018. Final Provincial approval was granted on May 7, 2018. The first term that we accepted enrollment applications was in the Fall of 2018. We accept applications on a rolling basis so students can begin the program and can graduate from the program in any term.

Enrolment to date:

- Currently 12 are registered in the diploma program
- 4 transferred to full time in the Master of Climate Change degree program at the University of Waterloo
- 2 withdrew from Diploma after completing some courses
- 7 have graduated with this GDip

Year	Number of Applicants	Number of Students Enrolled
2018-2019 (1st year)	10	5
2019-2020 (2nd year)	13	5
2020-2021 (3rd year)	25	12

Students enrolled in the program (total) by term of offer:

Term	Student count	Term	Student count	Term	Student count
F2018	3	F2019	4	F2020	12
W2019	4	W2020	8	W2021	9
S2019	5	S2020	7	S2021	11

Progress on Implementation

The Climate Risk Management (CRM) Diploma program has been implemented as planned. There have been only minor changes to the program structure or implementation plan as follows:

- The program no longer requires CRM students to take GEMCC 600 (Fundamentals of Climate Change) as the “first” course in the diploma. Students are not exempted from GEMCC 600 and must still complete it to graduate from the program. This relaxation means that students can enter the program in any of the three terms in the year.
- Some modifications to course instructors have been made on the basis of availability (some courses are taught by faculty members in other Departments/Schools and they determine instructor availability each year).

The program also continues to refine and add course offerings for CRM and other students as follows:

1. GEMCC 620 (Climate Data Analytics) has been completely re-designed based on student feedback and the availability of a new faculty complement with required expertise.
2. A sixth course, GEMCC 644 Climate Resilient Canadians and Health Systems, has been recently added and was developed by Health Canada.
3. It is anticipated that a seventh course on urban sustainability transitions will be offered. This is scheduled for development Winter 2022.

The Faculty of Environment hired a staff position to support Graduate Student recruiting in 2019. Some of this staff time has been made available to the CRM Dip program (together with the Master of Climate Change degree program). The academic year 2020-21 has seen 25 applications to the GDip in CRM indicating strong interest in the program.

The Covid-19 pandemic has not disrupted course offerings for this online program but has likely impacted enrollment numbers to some extent based on the number of deferrals the Master of Climate Change degree program experienced in Fall 2020.

The CRM diploma will undergo its first full cyclical program review in 2025-26. In the lead up to this review, the program has begun to conduct exit surveys of students who complete the program.

Recommendations

Type 3 Grad Diplomas qualify for expedited review, which means that there was no external review and thus no recommendations to report on.

Date of first program review: _____ **2025-26**
Date

Signatures of Approval:

Richard Judson Kelly

(Department Chair) 20 August 2021
Date

Dan Scott

(Program Director) 20 August 2021
Date

AFIW Administrative Dean/Head (For AFIW programs only) Date

Jean Aubrey

Faculty Dean 25 August 2021
Date

Note: AFIW programs fall under the Faculty of ARTS; however, the Dean does not have fiscal control nor authority over staffing and administration of the program.

Associate Vice-President, Academic (For undergraduate programs) Date

Jeff M. Casell

18 January 2022

Associate Vice-President, Graduate Studies and Postdoctoral Affairs (For graduate programs) Date

HEALTH GRADUATE STUDIES

October 14, 2022

TO: Members, Senate Graduate and Research Council
FROM: Aiysh Rajendram, Graduate Studies Administrator
RE: Motions

The attached Health Graduate motions were approved by the Health Faculty Council meeting on September 7, 2022 and are now being submitted for approval by the Senate Graduate and Research Council on October 17, 2022.

Aiysh Rajendram

Attach.

From: Faculty of Health Graduate Studies Committee (Sept 7, 2022)

To: Admin Council (Sept 14, 2022) for approval

Graduate calendar changes for Faculty of Health

1. PROGRAM CHANGES

1.1 School of Public Health Sciences* effective 2023

- 1.1.1 **Motion:** Converting one of the program's two on-campus block courses (HLTH 602A) into a full-term course.

Rationale: *HLTH 602A has been offered as an intensive two-week on campus course held prior to the start of the Fall term, with online follow-up assignments throughout the Fall term. However, the cost and inconvenience to students who need to travel to Waterloo during what for many is a holiday period, coupled with increasing pressures to include more substantive content to meet core competency requirements, has led the School to recommend changes to a full-term Fall course. Some of the orientation functions that the course once had will continue to be delivered, but during UW's orientation week, and will be available online.*

- 1.1.2 **Motion:** Updating the course description, changing the grading basis from credit/no credit to numerical for HLTH 602A.

Rationale: *HLTH 602A has been offered as an intensive two-week on campus course held prior to the start of the Fall term, with online follow-up assignments throughout the Fall term. However, the cost and inconvenience to students who need to travel to Waterloo during what for many is a holiday period, coupled with increasing pressures to include more substantive content to meet core competency requirements, has led the School to recommend changes to a full-term Fall course. Some of the orientation functions that the course once had will continue to be delivered, but during UW's orientation week, and will be available online.*

- 1.1.3 **Motion:** Adding HLTH 650 to the list of elective courses associated with the Graduate Research Field in Health Informatics.

Rationale: *There is an urgent need to conduct public health and population health research using artificial intelligence (AI) methods and assess the implications of greater AI adoption. Adding HLTH 650 "AI for Public Health" course to the list of electives would allow our graduate students to build the capacity necessary to take advantage of emerging AI approaches for population and public health research. It would further strengthen their quantitative analytics skills.*

- 1.1.4 **Motion:** Revising the title of the Associate Director, Graduate Programs.

***attachment**

Prior to form submission, review the [content revision instructions](#) and information regarding [major/minor modifications](#). For questions about the form submission, contact [Trevor Clews](#), Graduate Studies and Postdoctoral Affairs (GSPA).

Faculty: Health

Program: Master of Public Health (MPH)

Program contact name(s): Mark Oremus

Form completed by: Mark Oremus

Description of proposed changes:

Note: changes to courses and milestones also require the completion/submission of the [SGRC Graduate Studies Course/Milestone Form](#).

Converting one of the program's two on-campus block courses (HLTH 602A) into a full-term course.

Is this a [major modification](#) to the program? No

Rationale for change(s):

HLTH 602A has been offered as an intensive two-week on campus course held prior to the start of the Fall term, with online follow-up assignments throughout the Fall term. However, the cost and inconvenience to students who need to travel to Waterloo during what for many is a holiday period, coupled with increasing pressures to include more substantive content to meet core competency requirements, has led the School to recommend changes to a full-term Fall course. Some of the orientation functions that the course once had will continue to be delivered, but during UW's orientation week, and will be available online.

Note: the content in the "Current Graduate Studies Academic Calendar content" column includes material that was approved by SGRC on May 9, 2022 which takes effect Fall 2022.

Proposed effective date: Term: Fall Year: 2023

Current [Graduate Studies Academic Calendar \(GSAC\)](#) page (include the link to the web page where the changes are to be made):

<https://uwaterloo.ca/graduate-studies-academic-calendar/applied-health-sciences/school-public-health-sciences/master-public-health-mph>

Current Graduate Studies Academic Calendar content:	Proposed Graduate Studies Academic Calendar content:
<p>Program information</p> <ul style="list-style-type: none"> • Admit term(s) <ul style="list-style-type: none"> ○ Fall • Delivery mode <ul style="list-style-type: none"> ○ On-campus 	<p>Program information</p> <ul style="list-style-type: none"> • Admit term(s) <ul style="list-style-type: none"> ○ Fall • Delivery mode <ul style="list-style-type: none"> ○ On-campus

Current Graduate Studies Academic Calendar content:	Proposed Graduate Studies Academic Calendar content:
<ul style="list-style-type: none"> ○ Online • Delivery mode information <ul style="list-style-type: none"> ○ All students must attend (two) <u>two week</u> on-campus courses. Courses are available either on-campus, online, or in a blended/hybrid format. Students should check the School's website for the latest information for format and timing of the courses for the most current mode of delivery and offering. • Length of program <ul style="list-style-type: none"> ○ Full-time: 6 terms (24 months) ○ Part-time: 12 terms (48 months) ○ Courses are offered in three terms of each academic year. For all, continuous registration for each term of the program is required. • Program type <ul style="list-style-type: none"> ○ Master's ○ Professional • Registration option(s) <ul style="list-style-type: none"> ○ Full-time ○ Part-time • Study option(s) <ul style="list-style-type: none"> ○ Coursework <p>Degree requirements</p> <ul style="list-style-type: none"> • Courses <ul style="list-style-type: none"> ○ The minimum course requirements are 44 one-term (0.50 unit weight) graduate courses, 2 block courses requiring two weeks on campus (0.50 unit weight) and a practicum (1.50 unit weight). ○ Students will attend on-campus on two occasions for 2-week block courses. The first, HLTH 602A Foundations of Public Health, will occur at the start of the program and the second, HLTH 602B Capstone Integrative Seminar for Public Health, will bring students back together at the end of the program after completion of all coursework and the practicum: <ul style="list-style-type: none"> • The objective of HLTH 602A, the Foundations of Public Health course is to provide 	<ul style="list-style-type: none"> ○ Online • Delivery mode information <ul style="list-style-type: none"> ○ All students must attend <u>a two-day on-campus orientation session scheduled the week prior to the start of classes in the Fall term. In addition, a one-week on-campus capstone course is required at the conclusion of the program.</u> Courses are available either on-campus, online, or in a blended/hybrid format. Students should check the School's website for the latest information for format and timing of the courses for the most current mode of delivery and offering. • Length of program <ul style="list-style-type: none"> ○ Full-time: 6 terms (24 months) ○ Part-time: 12 terms (48 months) ○ Courses are offered in three terms of each academic year. For all, continuous registration for each term of the program is required. • Program type <ul style="list-style-type: none"> ○ Master's ○ Professional • Registration option(s) <ul style="list-style-type: none"> ○ Full-time ○ Part-time • Study option(s) <ul style="list-style-type: none"> ○ Coursework <p>Degree requirements</p> <ul style="list-style-type: none"> • Courses <ul style="list-style-type: none"> ○ The minimum course requirements are <u>12</u> one-term (0.50 unit weight) graduate courses, <u>1</u> block course requiring <u>one-week</u> on campus (0.50 unit weight) and a practicum (1.50 unit weight). ○ Students will attend on-campus on <u>one</u> occasion for <u>a 1-week</u> block course. <u>This course, HLTH 602B Capstone Integrative Seminar for Public Health, will bring students together at the end of the program after completion of all coursework and the practicum. HTLH 602B is a culminating integrated</u>

Current Graduate Studies Academic Calendar content:	Proposed Graduate Studies Academic Calendar content:
<p>students with foundational knowledge of public health, orient the student to the philosophical and practical bases of public health, and to kindle the student's passion for public health as a career and as a societal activity.</p> <ul style="list-style-type: none"> ▪ HTLH 602B, the final MPH capstone course, is a culminating integrated learning experience that provides a context for students to demonstrate their achievement of the foundational knowledge and core competencies of public health. On-campus workshops and preparation and presentation of a capstone project are required for the completion of this course. ○ Additional required courses are as follows: <ul style="list-style-type: none"> ▪ HLTH 603 Health Policy in Public Health ▪ HLTH 604 Public Health and the Environment ▪ One of: HLTH 605A Regression Models OR HLTH 605B Quantitative Methods and Analysis ▪ One of: HLTH 606A Epidemiological Methods OR HLTH 606B Principles of Epidemiology for Public Health ▪ HLTH 607 Social, Cultural and Behavioural Aspects of Public Health I ▪ HLTH 608 Health and Risk Communication in Public Health ▪ HLTH 609 Management and Administration of Public Health Services ▪ HLTH 617 Population Intervention for Disease Prevention and Health Promotion ▪ HLTH 618 Research Tools for Public Health Practice ▪ HLTH 640 Professional Experience Practicum ▪ Two elective HLTH courses. Note: Graduate courses from 	<p>learning experience that provides a context for students to demonstrate their achievement of the foundational knowledge and core competencies of public health. On-campus workshops and preparation and presentation of a capstone project are required for the completion of this course.</p> <ul style="list-style-type: none"> ○ Additional required courses are as follows: <ul style="list-style-type: none"> ▪ <u>HLTH 602A the Foundations of Public Health</u> ▪ HLTH 603 Health Policy in Public Health ▪ HLTH 604 Public Health and the Environment ▪ One of: HLTH 605A Regression Models OR HLTH 605B Quantitative Methods and Analysis ▪ One of: HLTH 606A Epidemiological Methods OR HLTH 606B Principles of Epidemiology for Public Health ▪ HLTH 607 Social, Cultural and Behavioural Aspects of Public Health I ▪ HLTH 608 Health and Risk Communication in Public Health ▪ HLTH 609 Management and Administration of Public Health Services ▪ HLTH 617 Population Intervention for Disease Prevention and Health Promotion ▪ HLTH 618 Research Tools for Public Health Practice ▪ HLTH 640 Professional Experience Practicum ▪ Two elective HLTH courses. Note: Graduate courses from other departments/schools may be acceptable if approved by the SPHS Professional Graduate Programs Committee ○ At a minimum, students must obtain an average of 75% or higher in aggregate on the courses presented in fulfilment of the degree requirements. Grades on all courses presented to fulfill the degree requirements must be 70% or higher. A grade below 70% in any

Current Graduate Studies Academic Calendar content:	Proposed Graduate Studies Academic Calendar content:
<p>other departments/schools may be acceptable if approved by the SPHS Professional Graduate Programs Committee</p> <ul style="list-style-type: none"> ○ At a minimum, students must obtain an average of 75% or higher in aggregate on the courses presented in fulfillment of the degree requirements. Grades on all courses presented to fulfill the degree requirements must be 70% or higher. A grade below 70% in any course or failing to maintain an average of 75% will necessitate a review of the student's status by the School of Public Health Sciences (SPHS) and may result in a student being required to complete additional coursework or being required to withdraw from the program. The School reserves the right to stipulate additional coursework if it is necessary for the student's preparation. ○ Students admitted for a probationary year will be required to complete HLTH 605A Regression Models (on-campus only) or 605B Quantitative Methods and Analysis (online, fall term) and HLTH 606A Epidemiological Methods (on-campus only) or HLTH 606B Principles of Epidemiology for Public Health (online, winter term) with an average of at least 73%. If a student's average on these courses falls below 73% but not below 70%, their status will be reviewed by the SPHS Professional Graduate Programs Committee. Normally a student will not continue on probationary status for more than two terms. 	<p>course or failing to maintain an average of 75% will necessitate a review of the student's status by the School of Public Health Sciences (SPHS) and may result in a student being required to complete additional coursework or being required to withdraw from the program. The School reserves the right to stipulate additional coursework if it is necessary for the student's preparation.</p> <ul style="list-style-type: none"> ○ Students admitted for a probationary year will be required to complete HLTH 605A Regression Models (on-campus only) or 605B Quantitative Methods and Analysis (online, fall term) and HLTH 606A Epidemiological Methods (on-campus only) or HLTH 606B Principles of Epidemiology for Public Health (online, winter term) with an average of at least 73%. If a student's average on these courses falls below 73% but not below 70%, their status will be reviewed by the SPHS Professional Graduate Programs Committee. Normally a student will not continue on probationary status for more than two terms.

How will students currently registered in the program be impacted by these changes?

This will not affect any students currently registered in the program. The revisions will come into place for those entering the program in Fall, 2023.

Department/School approval date (mm/dd/yy): 06/23/22

Reviewed by GSPA (for GSPA use only) date (mm/dd/yy): 06/14/22

Faculty approval date (mm/dd/yy): 09/30/2022

Senate Graduate & Research Council (SGRC) approval date (mm/dd/yy):

Senate approval date (mm/dd/yy) (if applicable):

Prior to form submission, review the [content revision instructions](#). For questions about the form submission, contact [Trevor Clews](#), Graduate Studies and Postdoctoral Affairs (GSPA).

Faculty: Health

Effective date: Term: Fall Year: 2023

Milestone

Note: milestone changes also require the completion/submission of the [Graduate Studies Program Revision Template](#).

- New: Choose an item.
- Inactivate: Choose an item.
- Revise: from Choose an item. to Choose an item.

Course

Note: some course changes also require the completion/submission of the [Graduate Studies Program Revision Template](#).

- New: Complete all course elements below
- Inactivate: Complete the following course elements:
Course subject code, Course number, Course ID, Course title
- Revise: Complete all course elements below to reflect the proposed change(s) and identify the course elements being revised (*e.g. Course description, Course title*):

Updating the course description, changing the grading basis from credit/no credit to numerical.

Course elements (complete as indicated above. Review the [glossary of terms](#) for details on course elements)

Course subject code: HLTH

Course number: 602A

Course ID: 012523

Course title (max. 100 characters including spaces): Foundations of Public Health

Course short title (max. 30 characters including spaces): Foundations of Public Health

Grading basis: Numerical

Course credit weight: 0.50

Course consent required: Department

Course description:

Current description: An introduction to the philosophical, historical, ecological, legislative, and ethical foundations for understanding the practice of public health in Canada. The course is delivered in a 2-week block at the beginning of the MPH program sequence on the UW main campus. For MPH student only. The course must be successfully completed by MPH students before proceeding to other courses in the MPH program sequence.

Revised description: Overview of the conceptual, theoretical, practical, and professional foundations of public health. The course will help students build an understanding of the historical origins and achievements of public health practitioners and establish an appreciation of the core values that underpin, and the core functions that make up, public health. Examination and analysis of current approaches to prevent, control, and manage the major causes of illness and disease worldwide. The course also serves as an introduction to the MPH program. As such, it is required to be taken in the first term of the MPH program.

Meet type(s): Lecture Choose an item. Choose an item. Choose an item.

Primary meet type: Lecture

Delivery mode: On-campus and also offered online

Requisites: Master of Public Health Students only.

Special topics course: Yes No

Cross-listed course: Yes No

Course subject code(s) and number(s) to be cross-listed with and approval status:

Sections combined/held with:

Rationale for request:

HLTH 602A has been offered as an intensive two-week on campus course held prior to the start of the Fall term, with online follow-up assignments throughout the Fall term. However, the cost and inconvenience to students who need to travel to Waterloo during what for many is a holiday period, coupled with increasing pressures to include more substantive content to meet core competency requirements, has led the School to recommend changes to a full-term Fall course. Some of the orientation functions that the course once had will continue to be delivered, but during UW's orientation week, and will be available online.

Form completed by: Craig R. Janes, Director and course developer (with CEL)

Department/School approval date (mm/dd/yy): 06/23/22

Reviewed by GSPA (for GSPA use only) date (mm/dd/yy): 06/14/22

Faculty approval date (mm/dd/yy):

Senate Graduate & Research Council (SGRC) approval date (mm/dd/yy):

Prior to form submission, review the [content revision instructions](#) and information regarding [major/minor modifications](#). For questions about the form submission, contact [Trevor Clews](#), Graduate Studies and Postdoctoral Affairs (GSPA).

Faculty: Health

Program: Doctor of Philosophy (PhD) in Public Health and Health Systems

Program contact name(s): Mark Oremus

Form completed by: Mark Oremus

Description of proposed changes:

Note: changes to courses and milestones also require the completion/submission of the [SGRC Graduate Studies Course/Milestone Form](#).

- 1) *Adding HLTH 650 to the list of elective courses associated with the Graduate Research Field in Health Informatics.*
- 2) *Revising the title of the Associate Director, Graduate Programs.*

Is this a [major modification](#) to the program? No

Rationale for change(s):

There is an urgent need to conduct public health and population health research using artificial intelligence (AI) methods, and assess the implications of greater AI adoption. Adding HLTH 650 "AI for Public Health" course to the list of electives would allow our graduate students to build the capacity necessary to take advantage of emerging AI approaches for population and public health research. It would further strengthen their quantitative analytics skills.

Proposed effective date: Term: Winter Year: 2023

Current [Graduate Studies Academic Calendar \(GSAC\)](#) page (include the link to the web page where the changes are to be made):

<https://uwaterloo.ca/graduate-studies-academic-calendar/applied-health-sciences/school-public-health-sciences/doctor-philosophy-phd-public-health-and-health-systems#health-informatics>

Current Graduate Studies Academic Calendar content:	Proposed Graduate Studies Academic Calendar content:
<p>Degree requirements</p> <ul style="list-style-type: none"> • Courses <ul style="list-style-type: none"> ○ 9 one-term graduate courses beyond the Bachelor's degree, including at least 4 courses (2 required and 2 electives) beyond the Master's degree, is the normal minimum requirement. 	<p>Degree requirements</p> <ul style="list-style-type: none"> • Courses <ul style="list-style-type: none"> ○ 9 one-term graduate courses beyond the Bachelor's degree, including at least 4 courses (2 required and 2 electives) beyond the Master's degree, is the normal minimum requirement.

Current Graduate Studies Academic Calendar content:	Proposed Graduate Studies Academic Calendar content:
<ul style="list-style-type: none"> ○ Required courses (2) <ul style="list-style-type: none"> ▪ HTLH 701 Interdisciplinary Seminar in Public Health and Health Systems ○ 1 of the following required methods courses: <ul style="list-style-type: none"> ▪ HLTH 704 Advanced Qualitative Methods for Health Research ▪ HLTH 705 Advanced Statistical Methods for Analyzing Public Health and Health Systems Data ▪ HLTH 706 Advanced Epidemiological Methods ▪ HLTH 719 Advanced Research Methods in Health Informatics ○ Elective courses (2) <ul style="list-style-type: none"> ▪ 1 methods elective course at the 600-or 700-level, selected in consultation with the supervisor (may include courses outside the SPHS), or courses offered by SPHS, including additional courses from the required course list. ▪ 1 additional elective, selected in consultation with the supervisor. Students without a background in public health and health systems, and focusing in research areas other than Health Informatics, should take HLTH 601 Lifespan Determinants of Health and Disease. Students focusing in Health Informatics may choose to take HLTH 611 The Health Care System or an equivalent course approved by the SPHS Graduate Officer. ○ Plus other free electives as may be required <ul style="list-style-type: none"> ▪ It is important to keep in mind that these are minimum requirements. Many students complete at least three courses within their area of research interest, which may require the addition of one or more extra courses to the minimum coursework requirement. ○ At a minimum, students must obtain an average of 75% or higher in aggregate 	<ul style="list-style-type: none"> ○ Required courses (2) <ul style="list-style-type: none"> ▪ HTLH 701 Interdisciplinary Seminar in Public Health and Health Systems ○ 1 of the following required methods courses: <ul style="list-style-type: none"> ▪ HLTH 704 Advanced Qualitative Methods for Health Research ▪ HLTH 705 Advanced Statistical Methods for Analyzing Public Health and Health Systems Data ▪ HLTH 706 Advanced Epidemiological Methods ▪ HLTH 719 Advanced Research Methods in Health Informatics ○ Elective courses (2) <ul style="list-style-type: none"> ▪ 1 methods elective course at the 600-or 700-level, selected in consultation with the supervisor (may include courses outside the SPHS), or courses offered by SPHS, including additional courses from the required course list. ▪ 1 additional elective, selected in consultation with the supervisor. Students without a background in public health and health systems, and focusing in research areas other than Health Informatics, should take HLTH 601 Lifespan Determinants of Health and Disease. Students focusing in Health Informatics may choose to take HLTH 611 The Health Care System or an equivalent course approved by the SPHS Graduate Officer. ○ Plus other free electives as may be required <ul style="list-style-type: none"> ▪ It is important to keep in mind that these are minimum requirements. Many students complete at least three courses within their area of research interest, which may require the addition of one or more extra courses to the minimum coursework requirement. ○ At a minimum, students must obtain an average of 75% or higher in aggregate

Current Graduate Studies Academic Calendar content:	Proposed Graduate Studies Academic Calendar content:
<p>on the courses presented in fulfillment of the degree requirements. Grades on all courses presented to fulfill the degree requirements must be 70% or higher. A grade below 70% in any course or failing to maintain an average of 75% will necessitate a review of the student's status by the School and may result in a student being required to complete additional coursework or being required to withdraw from the program. The School reserves the right to stipulate additional coursework if it is necessary for the student's preparation.</p> <ul style="list-style-type: none"> ○ Students in the PhD in Public Health and Health Systems program may also wish to pursue one of the following Graduate Research Fields: <ol style="list-style-type: none"> 1. Aging and Health 2. Epidemiology and Biostatistics 3. Global Health 4. Health and Environment 5. Health Evaluation 6. Health Informatics 7. Work and Health ○ A Graduate Research Field is a University credential that is recognized on the student's transcript and is intended to reflect that a student has successfully completed research and a set of courses that together provide an in-depth study in the area of the Graduate Research Field. A student will only obtain the Graduate Research Field on their transcript if they have completed the requirements associated with the PhD degree and the requirements associated with the Graduate Research Field. ○ All PhD Graduate Research Fields in the SPHS consist of a Comprehensive Examination, a PhD Thesis that is confirmed by the SPHS to be in the chosen Graduate Research Field, and a set of 4 graduate (0.50 weight) level courses. This set of courses is comprised of a mix of required and elective courses. Required courses are those that are prescribed as part of the Graduate Research Field. Elective courses are those that are on a list of 	<p>on the courses presented in fulfillment of the degree requirements. Grades on all courses presented to fulfill the degree requirements must be 70% or higher. A grade below 70% in any course or failing to maintain an average of 75% will necessitate a review of the student's status by the School and may result in a student being required to complete additional coursework or being required to withdraw from the program. The School reserves the right to stipulate additional coursework if it is necessary for the student's preparation.</p> <ul style="list-style-type: none"> ○ Students in the PhD in Public Health and Health Systems program may also wish to pursue one of the following Graduate Research Fields: <ol style="list-style-type: none"> 1. Aging and Health 2. Epidemiology and Biostatistics 3. Global Health 4. Health and Environment 5. Health Evaluation 6. Health Informatics 7. Work and Health ○ A Graduate Research Field is a University credential that is recognized on the student's transcript and is intended to reflect that a student has successfully completed research and a set of courses that together provide an in-depth study in the area of the Graduate Research Field. A student will only obtain the Graduate Research Field on their transcript if they have completed the requirements associated with the PhD degree and the requirements associated with the Graduate Research Field. ○ All PhD Graduate Research Fields in the SPHS consist of a Comprehensive Examination, a PhD Thesis that is confirmed by the SPHS to be in the chosen Graduate Research Field, and a set of 4 graduate (0.50 weight) level courses. This set of courses is comprised of a mix of required and elective courses. Required courses are those that are prescribed as part of the Graduate Research Field. Elective courses are those that are on a list of

Current Graduate Studies Academic Calendar content:	Proposed Graduate Studies Academic Calendar content:
<p>courses designated as electives for a given Graduate Research Field.</p> <ul style="list-style-type: none"> ○ Students who have completed the MSc in Public Health and Health Systems and obtained a Graduate Research Field can obtain the same or another Field or (by taking the applicable required/elective courses) as part of their PhD program. ○ For any of the Graduate Research Fields below, a directed studies course (HLTH 620 or HLTH 720) focused on the Graduate Research Field or an appropriate alternate course may replace a required or elective course, with the approval of the Associate Director, Research Graduate Program, School of Public Health Sciences. ○ The course requirements for the Graduate Research Fields are described below. <p>6. Graduate Research Field in Health Informatics</p> <ul style="list-style-type: none"> ○ Students must successfully complete 2 required courses and 2 elective courses. An assessment of whether or not the student's thesis warrants the Health Informatics Graduate Research Field designation will be completed by the SPHS. <ul style="list-style-type: none"> ▪ Required courses: <ul style="list-style-type: none"> ▪ HLTH 701 Interdisciplinary Seminar in Public Health and Health Systems ▪ HLTH 719 Advanced Research Methods in Health Informatics OR Equivalent ▪ Elective courses: <ul style="list-style-type: none"> ▪ Select 1 from the following list: <ul style="list-style-type: none"> ▪ HLTH 615 Requirements Specification and Analysis in Health Systems ▪ HLTH 616 Decision Making and Systems Thinking in 	<p>courses designated as electives for a given Graduate Research Field.</p> <ul style="list-style-type: none"> ○ Students who have completed the MSc in Public Health and Health Systems and obtained a Graduate Research Field can obtain the same or another Field or (by taking the applicable required/elective courses) as part of their PhD program. ○ For any of the Graduate Research Fields below, a directed studies course (HLTH 620 or HLTH 720) focused on the Graduate Research Field or an appropriate alternate course may replace a required or elective course, with the approval of the Associate Director, Graduate Programs, School of Public Health Sciences. ○ The course requirements for the Graduate Research Fields are described below. <p>6. Graduate Research Field in Health Informatics</p> <ul style="list-style-type: none"> ○ Students must successfully complete 2 required courses and 2 elective courses. An assessment of whether or not the student's thesis warrants the Health Informatics Graduate Research Field designation will be completed by the SPHS. <ul style="list-style-type: none"> ▪ Required courses: <ul style="list-style-type: none"> ▪ HLTH 701 Interdisciplinary Seminar in Public Health and Health Systems ▪ HLTH 719 Advanced Research Methods in Health Informatics OR Equivalent ▪ Elective courses: <ul style="list-style-type: none"> ▪ Select 1 from the following list: <ul style="list-style-type: none"> ▪ HLTH 615 Requirements Specification and Analysis in Health Systems ▪ HLTH 616 Decision Making and Systems Thinking in

Current Graduate Studies Academic Calendar content:	Proposed Graduate Studies Academic Calendar content:
<p>Health Informatics</p> <ul style="list-style-type: none"> ▪ HLTH 626 Analysis and Management of Health Information in Aging Populations ▪ HLTH 629 Information Visualization ▪ HLTH 633 Digital Health ▪ HLTH 637 Public Health Informatics <ul style="list-style-type: none"> ▪ Select 1 from the following list: <ul style="list-style-type: none"> ▪ COGSCI 600 Seminar in Cognitive Science ▪ CS 634 Security and Privacy for Health Systems ▪ CS 792 Data Structures and Standards in Health Informatics ▪ CS 846 Advanced Topics in Software Engineering: Topic 30 Software Engineering for Big Data ▪ SYDE 642 Cognitive Engineering Methods ▪ SYDE 644 Human Factors Testing 	<p>Health Informatics</p> <ul style="list-style-type: none"> ▪ HLTH 626 Analysis and Management of Health Information in Aging Populations ▪ HLTH 629 Information Visualization ▪ HLTH 633 Digital Health ▪ HLTH 637 Public Health Informatics ▪ <u>HLTH 650 Applied Machine Learning and Artificial Intelligence in Public Health</u> <ul style="list-style-type: none"> ▪ Select 1 from the following list: <ul style="list-style-type: none"> ▪ COGSCI 600 Seminar in Cognitive Science ▪ CS 634 Security and Privacy for Health Systems ▪ CS 792 Data Structures and Standards in Health Informatics ▪ CS 846 Advanced Topics in Software Engineering: Topic 30 Software Engineering for Big Data ▪ SYDE 642 Cognitive Engineering Methods ▪ SYDE 644 Human Factors Testing

How will students currently registered in the program be impacted by these changes?

Since this is an elective, there is no foreseeable impact on the students currently registered in the program. In addition, since our current students in the Health Informatics field should already take pre-requisite courses, there is no obstacle for a current student to take HLTH 650.

Department/School approval date (mm/dd/yy): 06/23/22

Reviewed by GSPA (for GSPA use only) date (mm/dd/yy): 05/06/22

Faculty approval date (mm/dd/yy):

Senate Graduate & Research Council (SGRC) approval date (mm/dd/yy):

Senate approval date (mm/dd/yy) (if applicable):