12241
EMERGING DISCIPLINES TASK FORCE

P. Davita and G. Comrie presented on the Briefing Report and accompanying historical context paper to outline the history of the emerging task force that is set out to govern and regular the skill profession that is expanding at an accelerated rate of change and the emerging practices that conclude with the motion presented today.

Moved by G. Boone, seconded by R. Subramanian:

1. That the progress report of the Emerging Disciplines Task Force (EDTF) and its task group on Communications Infrastructure Engineering (CIE) in C-532-2.10 Appendix A be received, and its recommendations considered.

2. That Council make a policy decision to "enlarge PEO's tent" to include emerging and non-traditional disciplines, subdisciplines, scopes of practice, and controlled acts that are deemed to be the practice of professional engineering within the meaning of the Professional Engineers Act, and to implement structures, mechanisms, processes, and programs to regulate their practice and practitioners in an effective manner and without delay.

3. Whereas Council in Feb 2002 passed a motion creating a Standing committee to effectively monitor emerging disciplines and propose

methods to integrate these into the Engineering profession as reproduced here:

• "Establish a permanent committee to monitor the qualifications and experience of applicants and job advertisements to identify new engineering disciplines, or, alternatively, task staff to do this;
• Apply the outlined process for defining a body of knowledge to identified new engineering disciplines;
• Promptly identify an area of exclusive practice for the licensed practitioners of any new engineering discipline and work with government to secure appropriate demand-side legislation.
• Implement enforcement processes in relation to new engineering disciplines with legislated exclusive scopes of practice;
• Examine a discipline-specific licensing model."

Be it Resolved, That Council implement the decision by PEO Council in Feb 2002 under President Sterling and moved by Bruno DiStefano, and, That the committee be known as the Emerging Engineering Disciplines Committee (EEDC), and, that the initial and with initial membership as outlined in C-532-2.10, Appendix C., and, be constituted as per the draft terms of reference in C-532-2.10, Appendix B, to be reviewed at the first meeting of the EEDC and to make changes as necessary within the context and purpose of this initiative.

5. That Council authorize the ex-budget expenditure of $10,000 in 2020 for the Committee's and Task Group's operation.

6. That Council approve the roster and 2020 workplan of the CIE / CSSE Task Group under the new Committee, as set out in C-532-2.10, Appendix D.

7. Contingent on Motions 2., 3., 4., 5., and 6. being passed, that Council stand down the Emerging Disciplines Task Force with thanks, upon appointment of the EEDC at a future meeting.

Moved by D. Brown, seconded by L. MacCumber:

That the motion be amended to strike motions 1 through 7 and insert:

1. Council tasks the Executive Committee to consider the EDTF report in conjunction with their work on the governance roadmap and the SPTF recommendations; and

2. That Council stand down the Emerging Disciplines Task Force.

AMENDMENT CARRIED

Briefing Note – Decision

C-532-2.8

EMERGING DISCIPLINES TASK FORCE -
REGULATION OF NON-TRADITIONAL ENGINEERING DISCIPLINES

Purpose: To establish mechanisms for effective regulation of emerging and non-traditional engineering disciplines, subdisciplines, and scopes of professional practice, including creation of a standing committee on emerging engineering disciplines that would replace the existing Emerging Disciplines Task Force (EDTF), and expansion of its CIE / CSSE Task Group.

Motions to consider: (requires a simple majority of votes cast to carry)

1. **That the progress report of the Emerging Disciplines Task Force (EDTF) and its task group on Communications Infrastructure Engineering (CIE) in Appendix A be received, and its recommendations considered.**

2. **That Council make a policy decision to "enlarge PEO's tent" to include emerging and non-traditional disciplines, subdisciplines, scopes of practice, and controlled acts that are deemed to be the *practice of professional engineering* within the meaning of the Professional Engineers Act, and to implement structures, mechanisms, processes, and programs to regulate their practice and practitioners in an effective manner and without delay.**

3. **That Council agree to create a standing committee to identify new engineering disciplines, subdisciplines, and scopes of professional practice to determine whether or not they constitute the practise of professional engineering within the meaning of Section 1 of the *Professional Engineers Act*, and if so, to guide the process for their effective regulation in the public interest.**

4. **That the new standing committee be known as the *Emerging Engineering Disciplines Committee (EEDC)* and be constituted as per the draft terms of reference in Appendix B, and with initial membership as outlined in Appendix C.**

5. **That Council authorize the ex-budget expenditure of $10,000. in 2020 for the Committee's and Task Group's operation.**

6. **That Council approve the roster and 2020 workplan of the CIE / CSSE Task Group under the new Committee, as set out in Appendix D.**

7. **Contingent on Motions 2., 3., 4., 5., and 6. being passed, that Council stand down the Emerging Disciplines Task Force with thanks, upon appointment of the EEDC at a future meeting.**

Prepared by: Peter DeVita, P.Eng., FEC, -- Chair, Emerging Disciplines Task Force

Motion Sponsor: Councillor Guy Boone, P.Eng.

Need for PEO Action

Engineering is fundamentally different from most other senior professions by virtue of its large number of scopes of professional practice and areas of specialization, which number in the hundreds. This should not be surprising, given that engineering is fundamentally applied science, and that scientific / technical knowledge and its application are expanding exponentially. The scopes of professional practice that are associated with traditional engineering activities – particularly those that are defined in legislation as requiring a licensed professional to sign, seal, or otherwise take responsibility for the work – are relatively well established from a regulatory point of view, and are generally well understood and accepted on the part of practitioners, their employers and clients, and PEO as the regulator. They are also supported by established academic programs that have been designed to prepare practitioners for them.

On the other hand, scopes of practice that are on the periphery of the core engineering disciplines, or are entirely new, are often not well understood or accepted by industry or the profession. In many cases, even their practitioners do not see their work as the practice of professional engineering because they do not enjoy exclusive scopes of practice that are enforceable, and are therefore not inclined to seek or maintain licensure.

Those who do seek licensure may face challenges convincing the regulator (PEO) that what they are doing constitutes the *practice of professional engineering*, or that it meets the licensing criteria for acceptable engineering experience. Even if they are graduates of accredited engineering programs, their knowledge and skill in the emerging discipline will not likely have been acquired in academia, but rather on the job. PEO's approaches to evaluating experience are evolving slowly to address this problem, but in recent years Council has heard numerous complaints about the challenges some applicants face – even in some of the more traditional engineering disciplines.

The fundamental question being raised by the Task Force in this briefing note is this: **What is PEO's commitment to "enlarging its tent" as a regulator?** (i.e., to including areas of applied science on the periphery of the traditional engineering disciplines within its regulatory umbrella)

This is far from a new question for PEO Council, as documented in an unpublished paper by PEO's former Editor of *Engineering Dimensions* and Director of Communications Connie Mucklestone entitled *Regulation of Occupations Allied to Engineering in Ontario: Historical Overview and Explanation of Terms* that traces the discussion back to 1952. In the late 1990s, Council debated whether or not to include the practice and practitioners of geoscience within its purview, as has been done by a majority of Canadian engineering regulators. In the end, Council's decision was not to include the geoscientists, and they were left to form their own professional licensing body: *Professional Geoscientists Ontario (PGO)*. Some consider this decision a missed opportunity for PEO. In 2002, Council again debated whether or not to license engineering technologists with limited scopes of engineering practice, and this time, the decision – based on a report of the Engineering Technologist Licensure Task Force - was "yes". That decision, albeit a long time in implementation because

of government delays, saved PEO from much of the turmoil and conflict experienced by PEO's counterparts in Alberta and BC over the same issue.

For the past thirty years, PEO has had an almost continuous succession of task forces that have considered the regulatory aspects of various emerging engineering disciplines and applied science disciplines that are allied to engineering. Their recommendations – many of which were accepted by Council - are particularly relevant here. These include:

(i) ***Committee for the Professional Registration of Geoscientists in Ontario****: 1989-1998*

(ii) ***Task Group on Emerging Engineering and Multidisciplinary Groups****: 1996*
Established in November 1996 as part of PEO's "Fundamental Review", this task group recommended the creation of an *Engineering Disciplines Task Group*.

(iii) ***Engineering Disciplines Task Group (EDTG)****: 1998-2002*
Established in March 1998 and chaired by Dr. Bruno DiStefano, P.Eng., this Task Group looked into regulation of then emerging areas of engineering practice, in particular software engineering, with a view to how PEO's licensing criteria and process could be modified to deal with their applicants for licensure more effectively and fairly. Council received its final report with recommendations on February 28th, 2002 and passed the following motion: ***That Professional Engineers Ontario***

- ***Establish a permanent committee to monitor the qualifications and experience of applicants and job advertisements to identify new engineering disciplines, or, alternatively, task staff to do this;***
- ***Apply the outlined process for defining a body of knowledge to identified new engineering disciplines;***
- ***Promptly identify an area of exclusive practice for the licensed practitioners of any new engineering discipline and work with government to secure appropriate demand-side legislation.***
- ***Implement enforcement processes in relation to new engineering disciplines with legislated exclusive scopes of practice;***
- ***Examine a discipline-specific licensing model.***

(iv) ***Technologist Licensure Task Force****: 1999-2002*

(v) ***Ontario Software Engineering Task Force (OSWET)****: 2000-2002*
On September 16th, 2000 Council established the *Software Engineering Task Force* to prepare a reasoned response to the CCPE – AUCC proposal to create a joint Software Engineering Accreditation Board (SEAB). The Task Force completed this task, but although the SEAB was never created, the engineering profession's ability to regulate the practice of software engineering remained in doubt. As a result, on March 26th, 2001 Council empowered OSWET to hold discussions with the Canadian Information Processing Society (CIPS) and other groups representing the information technology community regarding the possible licensing of applied computer scientists with the following motion:
That Council agree in principle to hold discussions that may lead to the licensing of other classes of applied scientist or technologist by our Association under our Act.

(vi) External Groups Task Force: 2002-2006

At the same meeting, Council determined that the review of the regulation of other applied scientists should be handled by a super task force, with OSWET and the Technologist Licensure Task Force as subcommittees. The motion passed was:

That Council create a super task force to study the public interest implications of alternative models for governing allied applied science practitioners.

As a result, OSWET became known as *External Groups – Software*, and its discussions with CIPS National and CIPS Ontario continued through 2006. The agreed upon goal of these discussions was to:

- Define the world of software practice and come to an understanding of common terms that describe this field;
- Define standards of practice;
- Determine if there are areas of practice that are amenable to licensing or certification.

A white paper was prepared and received by Council in June, 2004.

(vii) ***Emerging Disciplines Task Force (EDTF)****: 2008 - present*

To proactively embrace emerging disciplines is also a "watershed" decision that is fundamental to PEO's future as a regulator. With the rapid advances in applied science and technology, the number of new scopes of professional engineering practice can be expected to continue to increase. Many of these scopes of practice will embody significant risks to the public, and ought to be regulated. If PEO chooses not to embrace them and regulate them effectively, PEO will continue to lose relevance and influence as a regulator, and over time will regulate a smaller and smaller percentage of engineering activity. One can imagine a scenario in which PEO devolves to represent only those professional engineers in the traditional building-related engineering disciplines who must be licensed in order to practise them.

The engineering subdiscipline highlighted in much of this report – *Communications Infrastructure Engineering (CIE)*, or *Cyber Systems Security Engineering (CSSE)* as it is more commonly referred to – is probably the best example of an emerging discipline that requires effective regulation to protect the public from the severe consequences of system security breaches that are in the news on a weekly basis. These scopes of practice will inevitably be regulated in the public interest, and soon. PEO is clearly the best positioned and equipped entity to regulate CIE / CSSE, and much good work has already been done to prepare PEO to do so. But if PEO chooses not to embrace these and other emerging disciplines and scopes of practice, some other entity will be created to regulate them, and PEO's opportunity to do so will be lost forever.

As previously noted, PEO's current Task Force on Emerging Disciplines (EDTF) has been in existence since 2008. EDTF spawned two Task Groups to deal with *Nanomolecular / Nanomaterials Engineering (NME) and Communications Infrastructure Engineering (CIE)* respectively, both of which were declared by Council to be the *practice of professional engineering* in 2010. Both subgroups had original workplans consisting of two phases that included consulting with academic and industry, defining scopes of professional practice and core bodies of knowledge, and developing recommendations as to how PEO should regulate them effectively. The NME subgroup submitted a report on its Phase I work in April of 2010, and a final report at the conclusion of its Phase II work in November of 2013, after which the subgroup effectively disbanded. The CIE subgroup submitted its Phase I report in September of 2010, and the executive summary of a planned Phase II report as a progress report in November of 2013.

The CIE Task Group's Phase II work involved extensive consultation with industry and government agencies in the telecommunications sector regarding regulatory aspects of CIE and the need for licensure / certification of practitioners. Because of this work, an opportunity arose for the Task Group to conduct a pilot project on licensure of existing practitioners with varying backgrounds, many of who were employed by Bell Canada in its Core Networks Group. With the support of the Registrar and staff in the Licensing and Registration Department, a group of over 40 potential applicants for P.Eng. and Limited licences were triaged, and those that applied were monitored through the assessment process. In the course of this exercise, a number of new applicants with CIE /CSSE scopes of practice were licensed, and PEO's internal licensing processes were refined to deal with such applicants.

This work constituted a third phase of the CIE Task Group's work. It also involved extensive consultation and collaboration with external experts, including PEO licensees who are cyber security experts in the Canadian Computer Security Establishment (CSE, part of DND). In the process, much valuable information was learned concerning what PEO needs to do to regulate CIE / CSSE effectively, and how to deal proactively with new and emerging disciplines in general. As it turns out, to embrace an emerging or non-traditional discipline requires focused activities such as extensive external outreach that are not part of PEO's normal licensing protocols for established disciplines.

The work required to regulate CIE / CSSE effectively is far from done. The appended report outlines a number of steps that remain to be completed, including refining the scopes of practice / controlled acts, refining the core body of knowledge, and introducing curriculum components into accredited engineering programs that deal with security in general and cyber security in particular. For this reason, the CIE Task Group should be continued and revitalized as a working group under the proposed new standing committee.

Proposed Action / Recommendation

1) Make a Commitment in Principle to "Enlarge PEO's Tent"

This is the fundamental decision on which everything else in this Briefing Note stands: **to make a commitment to regulate emerging and non-traditional engineering disciplines, subdisciplines, and scopes of professional practice – and their practitioners – in an effective and timely manner.**

It has profound implications for most of the other major decisions facing PEO Council, including some related to recommendations in the recent external regulatory review. If PEO intends to include and regulate practitioners of scopes of engineering practice on the periphery of the traditional scopes of engineering practice, it must change certain aspects of its core regulatory rubric, processes, and programs. If, on the other hand, PEO is content to confine its regulatory purview to the well-established scopes of engineering practice, then less dramatic change is required.

One thing we have learned from PEO's past attempts to embrace emerging disciplines such as software engineering and nanomaterials engineering is that it is completely ineffective to declare scopes of engineering practice to be the *practice of professional engineering* without having in place concrete plans and resources to implement the changes necessary to integrate them in a timely and effective manner. In addition, a licence is only effective if it has well defined rights to practice that can be enforced. This typically requires demand-side legislation or other regulatory regimes that ensure the involvement of licensed practitioners in the work.

For these reasons, the fundamental decision as to whether or not to "enlarge PEO's tent" should be made before taking other actions in response to the external review, not after.

2) Replace EDTF with a Standing Committee on Emerging Engineering Disciplines

PEO needs to create a standing committee to identify emerging and non-traditional engineering disciplines, subdisciplines, and scopes of professional practice and guide the process for their effective and timely regulation by PEO. The new committee would succede the existing *Emerging Disciplines Task Force (EDTF)*, which would be stood down. History has demonstrated clearly that the work required to identify and incorporate emerging disciplines is not a one-time project suitable for a task force, but rather ongoing, and requiring a long-term commitment.

The proposed structure for the new Emerging Engineering Disciplines Committee is analogous to that of the Licensing Committee and the Professional Standards Committee, in that it would have the ability to spawn (with Council approval) task groups of limited duration to deal with specific disciplines, subdisciplines, and scopes of engineering practice that have been identified as falling within PEO's purview and are not presently being regulated effectively.

3) Launch the Next Phase of PEO's Pilot Project to Bring CIE / CSSE Fully Into PEO's Tent

As described in Appendix A, PEO has made substantial progress over the past several years at incorporating the CIE / CSSE scopes of practice and their practitioners into PEO's regulatory rubric. CIE / CSSE is our best example of an emerging engineering discipline, in that:

- It is truly emerging, and evolving rapidly;
- It is largely unregulated at the present time, and has few professional standards;
- Its existing practitioners have acquired most of their knowledge and skills on the job;
- Its leaders recognize the need for engineering discipline;
- It is of critical importance to the safety and well being of society.

Treating this emerging [sub]discipline as a pilot project has enabled significant accomplishments in terms of adapting PEO's licensing requirements and processes to accommodate applicants who would otherwise be "outliers" in our traditional admission system.

This initiative would provide for the continuance of the Task Group on *Communications Infrastructure Engineering (CIE) / Cyber Systems Security Engineering (CSSE),* with an expanded roster, under the new Committee.

It would further provide for the continuance of the pilot project to complete some of the outstanding work required, including:

- Revision of the CIE / CSSE Core Body of Knowledge (CBOK);
- Incorporation in accredited engineering programs of core knowledge components related to security in general, and cyber security in particular;
- Establishment of a CIE / CSSE specialist designation;
- Establishment of virtual CIE / CSSE practice working group consisting of all willing PEO licensees practicing in the field;
- Significant further outreach to industry, practitioners, government agencies, and academia;
- Determining what demand-side legislation is required at both the provincial and federal levels.

Next Steps (If Motions 2. through 5. are approved)

Motions 2. through 5. are presented separately for purposes of Council debate and possible refinement, but are essentially inseverable.

The foundational policy decision represented by Motion 2. is necessary, but not sufficient, to accomplish the intended objective (i.e., to facilitate the effective and timely regulation of emerging and non-traditional engineering disciplines, subdisciplines, and scopes of professional practice). By itself, Motion 2. is impotent.

Needless to say, if motion 2. is not passed, the remaining motions need not be considered. In the event that Council decides not to move forward with this initiative, practitioners in emerging and non-traditional areas of engineering practice may seek alternative regulatory mechanisms outside of PEO to enhance their professional status and ensure that the public interest is served.

Motions 3., 4., and 5. enable the constitution of the new Emerging Engineering Disciplines Committee (EEDC) which will meet, elect a Chair and Vice-Chair, and commence its work. Its first tasks will include:

- To review its Terms of Reference and recommend any changes to Council for approval;
- To prepare a Work Plan and HR Plan for 2020 for Council approval.

Motions 3., 4., and 5. provide the necessary framework for developing the Council decisions that must follow, such as:

(a) What specific areas of practice should be included in the "enlarged tent", and how they should be defined

Besides *Communications Infrastructure Engineering / Cyber Systems Security Engineering*, other examples for early consideration would include:

- ***Software Engineering***
- ***Industrial / Systems Engineering***
- ***Bio / Biomedical / Biomaterials Engineering***

These are suggested because:

- Council has long ago declared each to be the practice of professional engineering within the meaning of the Act;
- With the notable exception of CIE / CSSE, academia has already embraced them and our accredited engineering schools are already offering degree programs in them;
- PEO is not regulating a significant percentage of their practitioners at the present time;
- PEO does have a core base of licensed practitioners in each field on which to build.

(b) What changes are necessary to PEO's regulatory rubric, policies, programs, and procedures in order to embrace and regulate them

Based on the Task Group's experience to date with CIE / CSSE, PEO must undertake the following in order to achieve the objective of integrating emerging and non-traditional areas of practice:

- Careful definition of targeted scopes of practice (what work is included, and what isn't);
- Discipline-specific specialist designations;
- Outreach to industry and existing practitioners;
- Outreach to academia, including the colleges;
- Discipline-specific competency frameworks for experience evaluation.

Even more fundamental aspects of PEO's current regulatory rubric may need to be examined in order to deal appropriately with licensees in "marginal" areas of practice, such as graduates of accredited engineering programs working in management consulting, banking and finance, law, etc. Potential changes could include separating the title from the licence, and introducing new classes of licence or discipline-specific licences.

Motion 6. authorizes the reconstituted CIE / CSSE Task Group to continue its remaining work.

Policy or Program Contribution to PEO's Strategic Plan

These initiatives will contribute to the following three high-level objectives in PEO's 2018-2020 Strategic Plan:

- **Objective #3 – *Enhance PEO's public image***

  PEO will be seen by industry, governments, and practitioners as a leader in public protection for faithfully discharging its mandate to serve the public by addressing one of society's most serious threats to its security.

- **Objective #5 – *Increase influence in matters regarding the regulation of the profession***

  PEO will begin to fulfil its legislated mandate to regulate the whole practice of professional engineering, not just the traditional areas of practice which by most estimates account for significantly less than half of all engineering practice in Ontario.

- **Objective #6 – *Augment the Applicant and Licence Holder Experience***

  PEO will enhance its licensing outreach, criteria, and processes to more readily attract and include practitioners in non-traditional and emerging areas of practice. These would include our own engineering graduates, many of whom do not see PEO as relevant to their careers.

Financial Impact on PEO Budgets (for five years)

	Operating	Capital	Explanation
Current to Year End	$10, 000.	$	Funded from Reserves (Council discretionary funds)
2nd	$20,000.		To be included in 2021-2022 Operating Budget

		$200,000.	for operation of Committee and Task Group(s) To be included in 2021-2022 Capital Budget for Public Information Campaign
3rd	$30,000.	$200,000.	To be included in 2022-2023 Operating Budget for operation of Committee and Task Groups To be included in 2022-2023 Capital Budget for Public Information Campaign
4th and thereafter	$40,000.	$200,000.	To be included in 2023-2024 Operating Budget for operation of Committee and Task Groups To be included in 2023-2024 Capital Budget for Public Information Campaign

Human Resource Implications

As noted in Appendices B and C, the volunteer rosters of both the Emerging Engineering Disciplines Committee and the CIE / CSSE Task Group need to be expanded and refreshed. Since their inception, the Emerging Disciplines Task Force and its CIE Task Group have enjoyed the support of PEO's Manager of Policy, Jordan Max, who has contributed extensively to their administration, as well as their outreach and networking efforts. For their continued operation, equivalent staff support will be required on an ongoing basis at a level of approximately 1/4 FTE.

Peer Review & Process Followed

Process Followed	• Repeated attempts made during 2017-2018, 2018-2019, and 2019-2020 Council terms to make a presentation at a Council plenary session. • Briefing Note placed on Council agenda for March 20th, 2020 regular meeting
Peer Review	• Existing members of Emerging Disciplines Task Force (EDTF) and Communications Infrastructure Engineering (CIE) Task Group

Appendices

- Appendix A – Progress Report of Task Group on Communications Infrastructure Engineering (CIE)
- Appendix B – Draft Terms of Reference for Emerging Engineering Disciplines Committee (EEDC)
- Appendix C – Proposed Initial Roster of Emerging Engineering Disciplines Committee (EEDC)
- Appendix D – Roster and 2020 Work Plan of Reconstituted CIE / CSSE Task Group

Emerging Disciplines Task Force (EDTF)

Communications Infrastructure Engineering (CIE) Task Group

PROGRESS REPORT

1. Introduction and Overview

This is the third report of the *Communications Infrastructure Engineering (CIE) Task Group* of PEO's *Emerging Disciplines Task Force (EDTF)*.

Our first (Phase I) report was issued in July 2010. The Phase I report demonstrated the need for - and the public interest inherent in - the establishment of a CIE field of engineering practice in Canada. It attempted to define:

- the impacts associated with protection of communications infrastructure and other critical infrastructures dependent on communications infrastructure,
- the core body of knowledge that should be mastered for competent CIE practice, and
- the scope and limitations of that practice.

In response to the Phase I report, *Communications Infrastructure Engineering* was accepted by PEO's Governing Council as the practice of professional engineering in September 2010.

The principal purpose of the Task Group's Phase II work was to give real meaning to licences to practise in this field by identifying (i) scopes of exclusive practice in CIE, and (ii) actions necessary for PEO to regulate the practice of CIE effectively. Our goal was to answer the question:

> *"What will it take for the self-regulating engineering profession to embrace the practice of CIE within its regulatory fabric, and to establish itself as a leader in the protection of our society's critical communications and network-dependent infrastructures?"*

In its early days, the Task Group attempted to track and document the ever-increasing incidence of cyber security breaches with their associated vulnerabilities, attack vectors, mitigation strategies, and losses – but this proved to be an overwhelming task for a small group of volunteers. Fortunately, both public and private organizations have emerged in the burgeoning cyber security industry that investigate, track, and communicate such information for the benefit of those who are trying to protect their data and systems. Suffice it to say that the almost constant media coverage of cyber abuse is making the general public much more aware of the inherent risks to their privacy and security of our on-line way of life.

At its inception, the Task Group debated what to call the emerging discipline it was dealing with. The first iteration was *Communications Infrastructure and Networking (CIN)*, which soon gave way to just *Communications Infrastructure Engineering (CIE)*. Recently, the Task Group has debated at some length whether this nomenclature depicts adequately the nature and importance of the discipline. Most CIE practitioners would refer to what they do as *cyber security*, a term that more likely has meaning to members of the general public. As a result, we are leaning towards calling it *Cyber Systems Security Engineering (CSSE)*, as term that has gained acceptance in the U.S.

and other jurisdictions. Throughout this report, we will use the terms *CIE, CSSE, CIE / CSSE, and cyber security* interchangeably.

2) Stakeholder Consultations

Our initial step in Phase II was to consult extensively with interested stakeholders - both within and outside the engineering profession - to broaden our understanding of the environment in which CIE is taking place and to obtain their feedback on the concepts developed in our Phase I work. The Phase I report was distributed widely to a range of potential stakeholders, with a request for comments. The distribution was followed up with offers to meet with interested stakeholders to present PEO's position on CIE and to hear and understand their reactions. The following meetings / presentations were conducted, resulting in much useful feedback.

- PEO Academic Requirements Committee (ARC)
- PEO Experience Requirements Committee (ERC)
- PEO Enforcement Committee (ENF)
- PEO Professional Standards Committee (PSC)
- OCEPP Policy Engagement Series Presentation
- ISACA Golden Horseshoe Chapter
- Office of the CIO, Ontario
- Canadian Radio-Telecommunications Commission (CRTC)
- Industry Canada - ICT Sector Group
- Council of Ontario Deans of Engineering (CODE)
- Presentation to ITAC Cyber Security Forum
- Computer Security Establishment Canada (CSEC)
- Ontario MGS Communications Branch
- Canadian Internet Registration Authority (CIRA)
- Consulting Engineers Ontario (CEO) Board of Directors
- PEO Regulatory Committee Chairs
- Licensing Process Task Force (LPTF) re LEL Applicants (Sep 2013)
- Association of Power Producers of Ontario (APPrO) Panel on Cyber Security (Nov 2013)
- Bell Canada - Core Networks Group (Mar 2015)
- Engineering Innovations Forum Presentations on Cyber Security (Mar 2017)

3) CIE / CSSE Scopes of Practice

The first step in establishing a regulated profession is to define and delimit the activities for which a licence to practise is required in the public interest. Our Phase I report set the bounds for such activities within the CIE domain in terms of both network technology and level of responsibility. The Task Group then proceeded to define specific work activities that constitute professional CIE practice.

At a high level, Communications Infrastructure Engineering (CIE) may be defined as the systems-level design, implementation, management, analysis, and audit of assured or trusted communication networks. In this context, "trusted" includes concerns for availability, confidentiality, integrity and privacy. CIE deals with data in transit, as opposed to data in repository or at rest. It excludes configuration and troubleshooting of network devices such as routers and firewalls. It also excludes application-specific security concerns and provisions.

The practice of Communications Infrastructure Engineering is primarily a systems level practice that uses product level components developed by other engineering disciplines such as electrical engineering, computer engineering, and software engineering. This is analogous to structural engineers using materials developed by metallurgical or chemical engineers in their design of structures.

Our Phase I report attempted to define the bounds of CIE in terms of network technology / topology and the core network elements of data, physical infrastructure, logical infrastructure, and point of demarcation. It emphasized that CIE deals with data in transit, thereby excluding cyber security issues associated with end-point data repositories and application software. Finally, it excluded from the CIE scope definition activities that normally fall within the purview of network technicians and technologists, such as installation, configuration, and troubleshooting of routers and firewalls, for example.

Without limiting the generality of the foregoing definition, the following subsections describe some specific areas of practice within the field of CIE.

3.1 Planning and Design of Assured Communication Networks

By definition, assured communication networks include those supporting other critical infrastructures, as defined by the Government of Canada.[1] Any communications infrastructure whose failure, compromise, or unavailability can adversely affect society's well-being is critical, and must be secured against a broad spectrum of threats and failures.

The role of the CIE practitioner is concentrated at the systems level; i.e., it is concerned with the overall design of the network from the point of view of:

- *availability* (which encompasses performance) and reliability,
- *confidentiality* (protection against unauthorized access or exposure),
- *integrity* (protection against unauthorized modification/corruption, including "operations" security),
- privacy (restrictions on unauthorized disclosure),

1 Public Safety Canada, *National Strategy for Critical Infrastructure*, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf, 2009.

and includes the design of secure operating and monitoring procedures. It is not intended to encompass the configuration of network devices and interfaces (which is the purview of the network technician or technologist), nor is it intended to encompass the design of secure applications (which is the purview of the software analyst and/or designer). However, the CIE practitioner is expected to understand these works and take overall system responsibility for the work done.

CIE practitioners apply their engineering discipline – which includes comprehensive risk assessment and mitigation strategies – to develop and document requirements for network assurance and security, along with specifications and designs that will meet those requirements.

3.2 Implementation of Assured Communication Networks

As in most other engineering disciplines, there is a requirement for a licensed CIE practitioner to monitor, inspect / review, and provide oversight to the implementation of an assured network to ensure that it is implemented in accordance with its designs. In some cases, issues will arise during implementation that may require the design to be revisited and possibly revised. Any such reviews and revisions cannot be left to persons less skilled than the designer without risking compromise of the network security. Thus, CIEs are expected to be involved in implementation of their designs, just as other engineers are. A CIE should "sign off" on the “as-built” implementation of an assured network as verification that it may be trusted.

3.3 Operational Oversight of Assured Communication Networks

Just as a certified aircraft must be operated in accordance with its Pilot Operating Handbook to be flown safely, so a secure network that has been properly designed and risk assessed must be operated in accordance with documented operating procedures to avoid failure or compromise.

The role of the CIE practitioner in operation of critical communications infrastructure is to provide the oversight necessary to ensure that its operation is in accordance with design limitations and secure practices, and to ensure that those practices are updated as and when required to reflect any changes in the design or configuration of the network.

This role includes ensuring that monitoring facilities are in place to detect any compromises of the network, and that appropriate corrective action is taken to address any threats detected.

It is not intended to encompass routine day-to-day operation and control of networks (which is the purview of network operators), or repair and configuration of network devices (which is the purview of network technicians and technologists).

Again, however, the CIE practitioner must understand the fundamental technologies and be able to verify that implementation and maintenance work does not compromise the reliability and security of the network as originally designed.

3.4 Auditing and Risk Analysis of Network Infrastructure

As networks, network technology, and cyber-security threats are evolving rapidly, it will be necessary to evaluate existing network infrastructure on a regular basis to ensure that risks are properly identified and mitigated. Many existing networks were designed when technology was simpler and threats were fewer, without the end-to-end design undergoing formal risk analysis.

This scope of CIE practice emphasizes the critical engineering aspect of risk analysis in secure network design and operation. It also encompasses oversight of remedial analysis and contingency planning for corrective actions that may become necessary following a network failure or security breach.

3.5 Risk Analysis and Mitigation of Other Critical Infrastructure that is Dependent on Network Infrastructure

Since so much of society's critical infrastructure depends on network infrastructure, risk analysis and mitigation for infrastructures such as energy, finance, health care, public safety, and transportation will require knowledge of network infrastructure and its vulnerabilities. Communications infrastructure engineers will therefore be called upon to bring their specialized knowledge and skill to bear on designing, operating, and protecting other critical infrastructures.

Since the above scopes of practice were established, the Task Group has broadened somewhat its view as to what should be included in the CIE / CSSE scopes of practice. While we believe the focus should remain on networks and data in transit, it is difficult in cyber security practice, and probably unwise, to attempt to exclude data at rest (in storage) and data in use at network endpoints. With this in mind, a review and likely expansion of these scopes of CIE / CSSE practice is contemplated as a Phase IV activity.

4) CIE Practitioners

One of the challenges inherent in regulating a new engineering (sub)discipline like CIE is that its practitioners come from widely diverse backgrounds. Many lack formal education or training in their field of specialization, and have acquired their expertise solely through practical experience. In the case of CIE, academic programs that provide the required body of knowledge are just now being developed and introduced, and their graduates are few.

To this day, relatively few existing CIE practitioners have formal engineering or engineering technology backgrounds, and even fewer are licensed. This challenge is exacerbated by the fact that there exists currently an acute shortage of persons with the requisite CIE skill set in the labour market, and by the fact that there is as yet no agreed upon standard of knowledge and skill for them.

An important concept in the strategy to regulate an emerging discipline is that of *targeted domains*: industry sectors and application areas that are logical choices for regulation and restricted rights to practise. The most obvious target domains for CIE are those in which there is a "logical-kinetic" interface between the communications

network and a device or system that is already recognized as falling within the purview of licensed professional engineers. CIE target domains include networks used to control mission-critical and safety-critical systems such as those used in communications (e.g., carriers and network / internet service providers), power generation (e.g., nuclear), transportation (e.g., aircraft and train control), industrial processes (SCADA), and so on.

5) Phase II Recommendations

In November, 2013 the Task Group filed with PEO Council a summary report of its Phase II work containing the following recommendations, organized according to whom the Task Force believed should be responsible for their implementation. The current status of each recommendation is noted in the table.

	Recommendation	Current Status
	Admissions - Related Recommendations	
1	That the Academic Requirements Committee (ARC) create a Syllabus (as defined in Regulations) for CIE, in order to substantiate its core body of knowledge.	Completed (2015)
2	That the Experience Requirements Committee (ERC) begin to add to its roster licensees who are practising in the CIE field, in order to be able to staff CIE interview panels and to structure interviews of CIE applicants.	Completed (2015)
3	That the proposal for a Limited Licence in CIE set out in Appendix L, be referred to PEO's standing committees on Academic Requirements (ARC), Experience Requirements (ERC), and Legislation (LEC), and its Licensing Process Task Force (LPTF), for peer review with a view to its implementability, and with the intention of bringing recommendations to Council for approval in the near term.	Completed: LEL Regs amended in 2016
4	That PEO establish a voluntary CIE specialist designation available exclusively to its licensees who meet a CIE certification standard.	Pending
5	That PEO establish as an additional character requirement for CIE designees a formal security clearance to be completed and maintained at the request and expense of the applicant / licensee.	Pending
6	That PEO establish a general certification process that can be applied to CIE and other such emerging disciplines and areas of specialization.	Pending
7	That Council task the Licensing Process Task Force / Standing Committee on Licensure Policy with investigating the need to increase the academic requirement for licensure to the equivalent of five (5) years of academic study.	Abandoned
8	That the CIE knowledge base and associated elements of the licensing process updated to reflect technology and regulatory changes by a task force composed of CIEs a minimum of once every 5 years for the next 20 years.	In Phase IV Work Plan

	Recommendations Related to Protection of Rights to Practice	
9	That the Terms of Reference for the Enforcement Committee (ENF) be amended to ensure that members of the Committee have practical experience with CIE scopes of practice, the cyber security industry, and control of critical physical infrastructure.	Not Implemented
10	That enforcement activity against unlicensed CIE practitioners be phased in gradually, beginning with instances of work on networks used to control mission-critical / safety critical infrastructure, including the shared backbone networks of telecommunications service providers, and private backbone networks of financial and government institutions.	Not Implemented - Premature
11	That the Professional Standards Committee (PSC) create a professional practice guideline for CIE that outlines the core body of knowledge and applicable technical standards and government regulations.	Refused by PSC
12	That licensees not originally licensed in CIE who wish to practice in this area refer to the CIE Core Body of Knowledge, Syllabus, and Practice Guideline (when available) to determine the technical knowledge and skill requirements for CIE practice, in order for their self-assessment of competency to begin practising in the field.	Pending
13	That PEO, together with other Canadian engineering regulators, begin to draft and promote public policies regarding necessary credentials of CIE practitioners in critical target domains.	Discussed with Engineers Canada Board
	Recommendations for Execution by the Registrar	
14	That PEO engage with Ontario engineering faculties to acquaint them with the body of knowledge expected of CIE practitioners / applicants for licensure, and to encourage them to offer and to seek CEAB accreditation of academic programs that meet those expectations.	Ongoing, by Task Group
15	That the CIE curriculum and knowledge base include instruction in: • systematic approaches to risk management, and • development of business cases associated with security and assurance of systems.	Pending
16	That the following content requirements for accredited CIE programs be prescribed by the Canadian Engineering Accreditation Board: • Security / Safety (Syllabus 04-Soft-B3) • Networking & Communications (Syllabus 04-Soft-B10) • Safety Critical Systems (Syllabus 04-Soft-B14) • Telecommunications Engineering (Carleton syllabus)	Pending
17	That PEO's Licensing and Registration Department maintain contact with post-secondary academic institutions that offer courses, programs, and certificates in CIE-related subject matter so as to be in a position to advise both applicants and existing licensees as to where they may obtain necessary additional CIE knowledge and skills.	Ongoing, by Task Group

	Other Recommendations	
18	That PEO support CIE licensure with communication and promotion targeted at the executive level, so that awareness and appreciation of the value of the CIE is understood and business case development is facilitated from lower levels in the organization.	Recommended by Public Information Campaign Task Force
19	That, with respect to communication and stakeholder relations concerning CIE: • Clear objectives and success criteria be developed and approved by Council; • A communication and stakeholder relations master plan be developed for the regulation of CIE along the lines presented above; • A project manager be assigned full-time to manage the execution of the communication and stakeholder relations plan; and • Achievement of plan objectives be tracked, and the plan and resources adjusted as required to deal with shortfalls.	Not Implemented
20	That the Emerging Disciplines Task Group continue to engage key external stakeholders in regulation of CIE with a view to identifying opportunities for collaboration.	Ongoing, by Task Group
21	That PEO, either independently or through Engineers Canada, partner with the Information and Communications Technology Council (ICTC) to develop labour market intelligence related to CIE occupational profiles with a view to determining the backgrounds and qualifications of those currently practising in CIE scopes of practice.	Not Implemented
22	That Council strike a standing committee on Emerging Engineering Disciplines with composition and terms of reference as set out in Appendix C.	Pending

6) Licensing of CIEs

Late in 2014, the Task Group established contact with representatives of Bell Canada's Core Networks Group in Toronto. This national group, which includes a few licensed professional engineers, is responsible for the architecture of the carrier's backbone networks and their security. We were invited to deliver two presentations on CIE to their interested staff in March of 2015. Some staff participated remotely from offices in Montreal and Calgary, which raised the question as to whether PEO's counterparts in other provinces were also interested in licensing practitioners in this field.

As a result of these presentations, Bell listed the P.Eng. and LEL as preferred qualifications / designations for professional development of their network security staff. This meant that the Company would reimburse application and other (e.g., examination) fees for these licences, as well as a bonus upon being awarded the licence or credential.

This positive development resulted in the receipt of approximately 30 applications for licensure from Bell Canada employees in a short period of time. PEO's Licensing

and Registration staff were soon inundated with inquiries as to how these CIE applications would be treated, especially given that most of the applicants did not have typical engineering academic backgrounds.

In order to achieve consistency in messaging and in the handling of applications from CIE practitioners, an ad-hoc working group consisting of L&R staff and representatives of ARC, ERC, and the CIE Task Group was established to review and refine the internal application process. This work was spearheaded by then Manager of Registration Lawrence Fogwill, P.Eng., who had been assigned to handle inquiries from CIE applicants. ARC members (notably Drs. Bob Dony, P.Eng. and Barna Szabados, P.Eng.) worked on refining the academic assessments, while ERC members (notably Changiz Sadr, P.Eng. and David Kiguel, P.Eng.) did the same for the experience assessments.

In the process, they were able to take advantage of changes to Section 46, of O.Reg. 941 dealing with Limited Licences and the L.E.T. designation that came into force on July 1st, 2015. These long-awaited changes that originated with the Technologist Licensure Task Force in 2002 made it easier to for applicants to meet the academic requirements for a Limited Licence.

The results were a streamlined and consistent process, demonstrating that PEO's existing requirements for licensure could be applied fairly to applicants with the non-standard backgrounds typical of practitioners in an emerging discipline.

As a pilot project, the Bell applications were "triaged"[2] and their progress through the system tracked by Deputy Registrar Michael Price and the Chairs of EDTF and the CIE Task Group. This permitted us to identify [potential] delays and obstacles to licensure, whether attributable to the applicant and his / her circumstances or to the process itself. It also provided a good indication that the Limited Licence would be applicable to a majority of CIE / CSSE practitioners (given that, as already reported, most existing practitioners do not have formal engineering backgrounds, although most have some post secondary education with sufficient basic science and mathematics to master the CIE core body of knowledge). Special assistance in the triage effort was provided by Daksha Bhasker, CISSP, P.Eng., of Bell Canada (at the time, herself an applicant for licensure).

In March of 2016, Council approved the addition of Element 2.4 – *CIE Outreach and Licensure* to PEO's 2015-2017 Strategic Plan. As of this report date, some 150 PEO licensees whose scopes of practice are in the CIE / CSSE field have been identified by the Task Group.

7) Education and Development of CIEs

Over the past few years, the Task Group has expended significant effort on outreach to academia in an attempt to identify new engineering programs with relevant CIE / SCCE content. Given that there is a well-documented and publicized shortage of cyber security professionals in every developed country including Canada, it is somewhat surprising that so few specialist programs have emerged in our Canadian engineering and engineering technology schools.

[2] An initial assessment of the applicant's credentials to determine if he / she would be a likely candidate for (i) an unlimited [P.Eng.] licence, (ii) a Limited Engineering Licence, or (iii) no licence.

This opportunity has been discussed on multiple occasions with the Council of Ontario Deans of Engineering (CODE), as well as with representatives of its national counterpart (NCDEAS) and Ontario's Deans of Technology. Their response to the question of why academic programs related to CIE / CSSE were developing so slowly has been that demand among students has not materialized as expected.

Plenty of training programs exist at the more practical, hands-on end of the spectrum oriented towards networking technicians, but university-level programs with more conceptual content targeting network design and protection are still few and far between, even at the post-graduate level. Recognizing a critical shortage of technical expertise in this area, the Government of Canada has recently begun to stimulate development of centres of cyber security research and development in academic institutions.

In 2018, the Task Group was approached by representatives of Canada's *Computer Security Establishment (CSE)* in Ottawa. Part of DND, CSE is the federal government's leading internal authority on cyber security, and is responsible for auditing and advising on the security of important federal government systems. Our contacts in CSE – coincidentally all PEO [P.Eng.] licensees – had been tasked with identifying academic programs in cyber security in Canada, and assessing the extent to which they adequately prepare graduates for the kinds of work undertaken by CSE itself and by other organizations with similar stringent skill requirements.

During the past two years, the Task Group has held regular teleconference meetings with the CSE representatives and other stakeholders, who have provided invaluable assistance in identifying emerging international knowledge, training, and practice standards. As a result of these in-depth discussions, we have come to the conclusion that it is necessary to revisit both the core body of knowledge and the defined scopes of professional practice in CIE / CSSE in order to bring them up to date.

A further result of our involvement with CSE is recommendations to incorporate:

(i) Core material related to security in general in all accredited Canadian engineering programs (regardless of discipline);

(ii) Core material covering the basic concepts of cyber security in all accredited Canadian engineering programs in *Electrical Engineering*, *Computer Engineering*, *Software Engineering*, *Systems Engineering*, *Communications / Networking Engineering,* and related areas of specialization;

(iii) Programs and program options designed to prepare graduates for professional practice in CIE / CSSE in their undergraduate course offerings.

The rationale for these recommendations, which are recast in Section 9. below, is as follows:

(i) Every licensed professional engineer must be prepared to consider the security of the artifacts and/or systems he /she designs, operates, and manages, regardless of their nature. The day in which one can assume that no one will attempt to attack, compromise, or destroy one's work product is long gone. Every engineering graduate should understand the basic concepts of security, risk management, and asset protection, and should have developed the related (technology-dependent) practice skills in his / her area of specialization.

(ii) These days, virtually all mission-critical / safety-critical devices and systems are interconnected, monitored, and controlled using internet protocol (IP) network technology, and are thus vulnerable to a wide range of cyber attacks. Those responsible for the design of such systems, regardless of their specific scopes of practice and technical specialization, need to have a basic understanding of the principles of cyber security, including vulnerability /threat assessment, attack vectors, and prevention / mitigation strategies in order to adequately protect the public. All undergraduate programs in the electrical /computer space should have this basic content.

(iii) The demand for cyber security specialists to will continue to grow exponentially. As detailed in the Task Group's Phase I report, the security of Canada's critical infrastructure will depend on sufficient supply in this segment of the labor market.

Most recently, the Task Group has obtained the assistance of a PEO licensee working with the US Military who has developed training materials for use in upgrading the cyber security skills of technical personnel in less developed countries. These materials should prove helpful in delivering basic cyber security competencies to existing practitioners who have not been exposed to them previously through their formal education / training.

8) Further Work Required

Despite its limited resources, and minimal support as a priority by PEO Council, the CIE Task Group has attempted to maintain momentum in its work to preserve for PEO the opportunity to take a leadership role in regulating this critical area of professional practice. The Task Group wishes to recognize the strong support it has received for our work from a relatively small but committed cadre of licensees who are practicing in the CIE / CSSE space, and who constitute the base for a discipline-specific practice committee / working group. The Task Group intends to continue its earlier attempts to pilot a virtual discipline-specific practice committee in order to assess the viability of this approach to obtaining input on regulatory issues and concerns specific to the discipline.

As previously noted, the following substantive items remain in the Task Group's Work Plan for 2020 (set out at Appendix D) and beyond:

8.1 Reconsideration of name of [sub]discipline

8.2 Review and extension of [sub]discipline definition and scopes of practice

8.3 Review and refinement of core body of knowledge

8.4 Ongoing consultation with academia regarding new programs and options

8.5 Consultation with CEAB concerning amendments to accreditation criteria

8.6 Development of a certification proposal for CIE / CSSE practitioners

9) Phase III Recommendations

9.1 **That PEO agree in principle to a voluntary CIE / CSSE specialist designation to be available exclusively to its licensees who meet a certification standard to be developed by the Task Group / Committee.**

9.2 **That PEO formally request the Canadian Engineering Accreditation Board (CEAB) to amend its accreditation criteria to include the following:**

- **(i) Core material related to security in general in all accredited Canadian engineering programs (regardless of discipline);**
- **(ii) Core material covering the basic concepts of cyber security in all accredited Canadian engineering programs in *Electrical Engineering*, *Computer Engineering*, *Software Engineering*, *Systems Engineering*, *Communications / Networking Engineering,* and related areas of specialization.**

9.3 **That PEO support CIE / CSSE licensure with communication and promotion for target industries and practitioners, as recommended by the Public Information Campaign Task Force (PICTF).**

Terms of Reference
Emerging Engineering Disciplines Committee (EEDC)

Issue Date: **Review Date:**
Approved by: **Review by:**

Legislated and other Mandate approved by Council	To identify potential new engineering disciplines, subdisciplines, and scopes of professional practice to determine whether they meet the definition of the *practice of professional engineering* set out in section 1 of the Professional Engineers Act, and if so, to guide the process for their regulation
Key Duties and Responsibilities	1. Maintain a continuous horizon watch for new and emerging areas of engineering practice that may fall within PEO's legislated mandate to regulate the practice of professional engineering. 2. With approval of Council, establish working groups (sub-committees or task groups) of specialists as necessary to investigate and report on new areas of engineering practice that appear to fall within PEO's regulatory mandate by virtue of a demonstrable need to protect the public interest. 3. Advise Council on how to resolve issues related to the growth in the number of new engineering disciplines, subdisciplines, and scopes of professional practice, including recommendations on possible new governing structures and their implications. 4. Work with PEO committees and staff to identify and support "communities of practice[3]" in the newly identified discipline(s) 5. Advise Council on what how to regulate effectively disciplines that are in common practice today but have limited or even no rights to practice associated with them. 6. Establish and maintain documentation on processes and best practices for assessing emerging and non-traditional disciplines and for establishing appropriate regulatory environments for them. 7. Maintain dialogue with Engineers Canada and its Constituent Associations and boards (CEAB and CEQB) on issues related to emerging and non-traditional engineering disciplines. 8. Work with ARC and CEAB to define and maintain a Core Body of Knowledge for each emerging engineering discipline. 9. Outreach to industry, government agencies, and academia as necessary with respect to their involvement in emerging and non-traditional engineering disciplines, subdisciplines, and scopes of professional practice. 10. Continue the Communications Infrastructure Engineering (CIE) Task Group as a sub-committee of this Committee.

[3] 'community of practice" is a group of people who share a concern or a passion for something they do, and learn how to do it better as they interact regularly. (source: http://wenger-trayner.com/resources/what-is-a-community-of-practice/)

Constituency & Qualifications of Committee/Task Force Members	A maximum of ten (10) members on the Main Committee itself. The Main Committee must have at least five (5) members to operate and will request additional members if membership falls below this. Each task / working group established under the Committee will be chaired by a Vice Chair of the Committee, and will have additional members appointed for the term of the task / working group from amongst members of the Committee and others chosen for their expertise and/or interest in the discipline under consideration. Committee members should have knowledge of and experience with professional engineering practice and at least one PEO regulatory committee such as ARC, ENF, ERC, LEC, LIC, or PSC. Preference will be given to committee members with experience in emerging and non-traditional scopes of engineering practice.
Qualifications and election of the Chair	Extensive knowledge of PEO's regulatory processes acquired through volunteering on one or more of PEO's regulatory committees Broad knowledge of engineering practices, including engineering research, design, development, and teaching. Election method to be determined by the committee; result presented to Council for approval
Qualifications and election of the Vice Chair(s)	Knowledge of PEO's regulatory processes Knowledge of engineering practices, and engineering research, design, development and practices. Election method to be determined by the committee and result presented to Council for approval
Duties of Vice Chair(s)	To chair meetings of the main Committee in the chair's absence, and to provide orientation and training for new members. To chair meetings of their respective working / task groups.
Term Limits for Committee members	A term on this Committee is three (3) years. A member may be re-appointed to an additional second term. There must be at least a one-year gap before coming back for additional appointments to this committee.
Quorum	Following the spirit of Wainberg's Society Meetings Including Rules of Order *and section 25(i) of By-Law No. 1, Quorum of the main Committee is 5 members or 50% of the Main Committee whichever is less.*
Approvals	Task group decisions are not binding on the main Committee and require approval of the main Committee for taking actions such as advising Council.

Meeting Frequency & Time Commitment	The Committee will hold at least four regular meetings per year, one in each calendar quarter, for at least one hour at a time. Additional regular or special meetings may be scheduled at any time with the agreement of the members. Ideally, participation will be in person, but teleconferencing/ videoconferencing is available as an option. Mutually convenient times will be determined by the Chair consulting with the committee members.
Operational year time frame	January – December
Committee advisor	To be determined by the Registrar

Emerging Engineering Disciplines Committee (EEDC)

INITIAL ROSTER

Existing members of EDTF, for continuity

- **George Comrie, P.Eng., CMC**
- **Peter DeVita, P.Eng.**
- **Roger Jones, P.Eng.**
- **Changiz Sadr, P.Eng**.

Four (4) additional members selected from the ranks of PEO licensees with emerging or non-traditional scopes of professional practice

One (1) sitting PEO Councillor (as Council Liaison)

Reconstituted CIE / CSSE Task Group

WORK PLAN - 2020

C-532-2.8
Appendix D

Approved by Committee: 28 February 2020		**Review Date:**	
Approved by Council:		**Approved Budget**:	
Mandate [as approved by Council]:	Task Group created pursuant to mandate of Emerging Engineering Disciplines Committee (EEDC), and Key Duty /Responsibility 2.: *With approval of Council, establish working groups (sub-committees or task groups) of specialists as necessary to investigate and report on new areas of engineering practice that appear to fall within PEO's regulatory mandate by virtue of a demonstrable need to protect the public interest.*		
Terms of Reference [Key duties]:	1. Identify issues relevant to PEO in the area of practice; 2. Define scopes of practice / controlled acts to be regulated; 3. Define core body of knowledge required for competent practice; 4. Investigate and make recommendations re academic programs related to the area of practice. 5. Make recommendations regarding licensing of practitioners; 6. Make recommendations regarding establishment and enforcement of rights to practice; 7. Evaluate existing and proposed certification programs as they may relate to PEO's responsibility to regulate the practice. 8. Outreach to practitioners, industry, government agencies, and academia as required, and develop external relationships where appropriate.		
Tasks, Outcomes / Deliverables, and Success Measures	**Tasks / Activities**	**Outcomes / Deliverables / Success Measures**	**Due Date**
	1. Work with other PEO committees (ARC, ERC, LIC, ENF, PSC) on licensure issues	Provide support to the other committees to implement CIE / CSSE licensure and regulation	As required
	2. Complete external stakeholder consultations for licensure issues; Gather market intelligence	Document stakeholder perspectives;	As required
	3. Provide Registrar with critical implementation factors for PEO to regulate CIE / CSSE	PEO secures substantive stakeholder agreement for implementation	As required
	4. Identify existing P.Eng.s practising CIE / CSSE, call for volunteers for PEO regulatory committees and establish a "Community of Practice" for CIE	Existing P.Eng.s. identified (voluntarily or through CPD practice questionnaire) At least 3 volunteers recruited for committees CIE Community of Practice established	June 2018

	5. Update the CIE Core Body of Knowledge	CIE CBOK updated	December 2020
	6. Develop Certification / Specialist Designation for CIE	Designation requirements and approval process developed for Council approval	December 2020
	7. Resolve nomenclature for CIE / CSSE discipline	Agreement on terminology	June 2020
Inter-committee collaboration:	Academic Requirements, Experience Requirements, Licensure, Professional Standards, Enforcement, Government Relations - consulting on proposals, presenting at committees		
Stakeholders:	• Engineers Canada and its constituent associations and boards (CEAB, CEQB) • Telcos and ISPs • Electricity generators and distributors, IESO, APPrO • Industry • Ontario universities and colleges of technology • Consulting Engineers Ontario, OACETT, OSPE • Ontario Ministries of Attorney General, Government Services, Research & Innovation, Health & Long-Term Care, Economic Development and Trade • Canadian Standards Association, Canadian General Standards Board • Information and Communications Technology Council (ICTC) • Industry Canada • Public Safety Canada • Department of National Defense, Computer Security Establishment • Public Works and Government Services Canada • Transport Canada • RCMP, CSIS, CBSA • CRTC, ITU, ITAC, CATA, CIRA • ISACA, ISSA, IEEE, IETF, ACM, Institution of Engineering and Technology • International Information Systems Security Certification Consortium (ISC)$_2$ • International Standards Organization • Ontario Information & Privacy Commissioner • Ontario Provincial Police, Emergency Management Ontario		

Reconstituted CIE / CSSE Task Group

ROSTER - 2020

- Daksha Bhasker, P.Eng.
- George Comrie, P.Eng., CMC
- Peter DeVita, P.Eng.
- Tyson Macaulay, LEL
- Parisa Mahdian, P.Eng.
- Mike Rowland, P.Eng.
- Changiz Sadr, P.Eng.
- Larry Stoddard, P.Eng.