

PUBLIC SECTOR CHIEF INFORMATION OFFICER COUNCIL (PSCI OC) VIRTUAL MEETING

September 23, 2020

Record of Decision v2

Attendance

PSCI OC Co-Chairs

Denis Skinner	Treasury Board of Canada Secretariat
Tracy Wood	Prince Edward Island

PSCI OC Members

Ryan Agar	Yukon (representing Sean McLeish)
Kathryn Bulko	MISA Canada (City of Toronto)
Dafna Carr	Ontario
Natasha Clarke	Nova Scotia
Gerry Fairweather	New Brunswick
Dave Heffernan	Newfoundland and Labrador
Stuart Hendrie	MISA East (Niagara Region)
CJ Ritchie	British Columbia
Pierre E. Rodrigue	Québec
Marty Robinson	MISA West (City of Medicine Hat)
Bonnie Schmidt	Saskatchewan
Dean Wells	Nunavut
Rick Wind	Northwest Territories
Munna Zaman	Manitoba

PSCI OC Observers

Tareq Al-Shumari	Ontario
Danielle Bourgon	Treasury Board of Canada Secretariat
Alex Bourque	Treasury Board of Canada Secretariat
Teresa D'Andrea	Treasury Board of Canada Secretariat
Keith Douglass	New Brunswick
Elky Hanlon	Nova Scotia
Ted Hickey	Nunavut
Zelko Holjevac	Ontario
Patrick Lagioia	Treasury Board of Canada Secretariat
Mark Levene	Treasury Board of Canada Secretariat

Robert Loughlin Gary Perkins Dawn Pilgrim Alexandra Underhill Meghan van Gall Erica van Wyngaarden Paul Wagner Dan Batista Sophia Jesow	New Brunswick British Columbia Ontario Canadian Centre for Cyber Security Treasury Board of Canada Secretariat Treasury Board of Canada Secretariat Treasury Board of Canada Secretariat Executive Director, ICCS JC Research Analyst, ICCS
ICCS Secretariat	
Maria Luisa Stefania Silisteanu	Director, National Councils (PSSDC & PSCIOC) Coordinator, National Councils (PSSDC & PSCIOC)

Item	Topic / Discussion	Decision / Action
1.	<p>Administrative Matters</p> <p>A) Approval of Record of Decision from February 26, 2020 in-person meeting in Toronto. Record of Decision of PSCIOC meeting of February 26th, 2020 adopted without changes.</p> <p>B) Approval of the September 23, 2020 PSCIOC meeting agenda. PSCIOC meeting agenda of September 23, 2020 approved.</p> <p><u>Other Business:</u></p> <p>A) PSCIOC Treasurer's Report (TAB C) Bonnie Schmidt, PSCIOC Treasurer, presented the PSCIOC final statement for information. No questions raised.</p> <p>B) PSCIOC Action Items from previous meeting (TAB D) – Tabled for information, no questions raised</p> <p>PSCIOC Bring Forward Agenda (TAB E) – Tabled for information, no questions raised</p> <p>C) Update Reports from PSCIOC Working Groups - The working group reports were included in the binder for information only.</p> <ul style="list-style-type: none"> Kathryn Bulko, IT Procurement Community of Practice Chair, advised that the group had not met since the start of the pandemic. This was partly due to her deployment to another role and that the CoP members were quite busy dealing with other priority issues. A report on the status of the group can be provided at a future PSCIOC meeting. Tracy Wood added that the Microsoft Office 365 Chair is looking to connect with the IT Procurement CoP for better alignment of work related to Microsoft. Kathryn Bulko confirmed that Maria Luisa Willan, Director, National Councils and Zelko Holjevac, MS O365 Working Group Chair, have already met to discuss groups' mandates. She advised that Zelko will be invited to future meetings of the IT Procurement CoP. 	<p><u>Decision #1:</u> Record of Decision of February 26, PSCIOC meeting in Winnipeg approved without changes.</p> <p><u>Decision #2:</u> Agenda of September 23, 2020 PSCIOC meeting approved.</p> <p><u>Action Item #1:</u> IT Procurement CoP to provide an update on the group's work at a future PSCIOC meeting.</p>

	<ul style="list-style-type: none"> ○ Next PSCIOC meeting: February 24th, 2021 (the in-person meeting in February is likely to be a virtual meeting due to the pandemic). <p><u>Tracy Wood asked for members' feedback on the Joint Councils virtual meeting of September 22nd.</u></p> <ul style="list-style-type: none"> • Robert Loughlin (NB) stated that meeting virtually is the common practice now and that it was efficient. • Natasha Clarke (NS) noted that the Joint Councils meeting was very well orchestrated, the ICCS did a great job, she knows how much work happens in the background to make this happen. This is moving in the right direction and it likely that more of Councils' business will be managed virtually in the future. She is thrilled about the level of engagement at the JC meeting versus the traditional teleconferences format. The content and flow went really well; however, she misses the impromptu meetings with colleagues when meeting in person. She noted that there are other offline meetings and discussions that happen when meeting in person and feels that this is a missed opportunity to connect. The virtual meeting went really well but still expect to meet in person in the future as well as virtually to maintain the level of engagement. • Rick Wind (NT) stated that there is a lot of value in the networking that happens at the in-person meetings, however, he found the virtual format engaging and seamless. 	
2.	<p>MICROSOFT (TAB 2)</p> <p>Tracy Wood welcomed John Hewie and his team from Microsoft and thanked them for making the time to meet with members of PSCIOC. She noted that members are looking forward to having a collaborative discussion on fostering a pan-Canadian strategic relationship between the jurisdictions as an FPTM table and Microsoft.</p> <p>John Hewie, National Security Officer, Microsoft, thanked PSCIOC members for the invitation and noted that his team is also interested in engaging the Council on discussions and/or opportunities for governments to be successful in their digital transformation initiatives and to help gain knowledge and reduce duplication of efforts across jurisdictions.</p> <ul style="list-style-type: none"> ○ John Weigelt, Chief Technology Officer for Microsoft in Canada, working across public sector and enterprise from the smallest to the largest organization, helping them to transform the technology and working on the interface between policy and technology. He spent lots of time in security, privacy and lately responsible application of Artificial Intelligence. He leads the Microsoft Canada AI team and he was a principal co-author of the Canada National Standard AI ethics and design and deployment of systems. ○ Cory Freed, Lawyer, supports public sector and commercial business, involved in contract negotiations and other legal matters ○ Celia Blakey, Licensing Executive specialized in licensing, negotiating contracts between Microsoft and the Crown. <p>In his remarks, John Hewie outlined the work of Microsoft Cloud which is a global service. In Canada, they have two regions, and they had some expansions of those regions recently in terms of enhanced availability zones, capacity and resiliency capabilities for customers. They design and operate Cloud services and have in a consistent manner everywhere in the world to meet the most robust security and privacy standards. They don't do unique things per region;</p>	<p>Action Item #2: Microsoft O365 WG Chair, Zelko Holjevac, to follow up with John Hewie, Microsoft, on the meeting discussion outcomes and report back to PSCIOC at a future meeting.</p>

Microsoft design as per higher standards around the world and that allows them to meet regional standards in different countries. The only exception here in Canada is working with the Treasury Board of Canada and Canadian Centre for Cyber Security so Microsoft have understood their requirements and the requests to have the Canadian data centres approved for document safeguarding at the protected B level. They streamed the local employees operating in those facilities to Canadian screening standards. Those individuals don't have any access to data, they are facilities management. All the support associated with the Cloud support happens from outside Canada. Most jurisdictions across Canada have an agreement with Microsoft and it is important to note that the way that they deliver, they deliver the exact same service to all those jurisdictions regardless of specific requirements within contracts. They've done some minor tailoring in those contracts to meet unique requirements, i.e. certain legislative or privacy nuances that are different between various jurisdictions.

Discussion on a minimal / baseline government plan which contains the essential products and services needed to stand up an O365 tenant as a Minimum Viable and Secure Product (MVSP) for Canadian public sector entities:

Tracy Wood (PEI) noted that at a pan-Canadian level the PSCIOC is seeking to ensure that they are leveraging the learnings in the work and the value that the jurisdictions receive through their contracts and their partnerships with Microsoft to help all jurisdictions to move forward at a faster pace. They want to maximize value and they don't want to duplicate efforts. It is a good starting point to have a robust conversation to move forward. They would like to discuss the product that they have, Office 365, to ensure that they have a minimum viable product and that is already existing in terms of the security provided around the world but sometimes the intricacies come when each jurisdiction is setting up their own configuration.

Zelko Holjevac, Microsoft Office 365 Working Group Chair, stated that members of his group are doing the same exercise to figure out what is exactly what they need for their environment. They understand that there is a uniqueness within each infrastructure and requirements. At the end of the day everybody does the same assessment, go to figure out is it O365, E1, E3, E5 and the components of those different categories. They try to peel away all the complexities around licensing and what jurisdictions may need. It is important to come together and talk about what is the SKU that they all need that account for security, privacy, productivity, collaboration, all those key activities that can be unique across the board in all jurisdictions. Having a discussion with Microsoft to see what opportunities there are across all jurisdictions in seeing how the Canadian government SKU looks like. They can go and learn about something else, but that foundational or base layer has been established for them because of the experience they've gained in moving to O365.

John Hewie noted that Ontario has been a leader. Mohammed Qureshi presented to some of their CISO Councils events. One of the programs that John Hewie runs and tries to share some of the programs across the country. They would like to scale some learning education around different capabilities, and they try to simplify licensing. The challenge is that Microsoft has a global set of customers and there are unique requirements. There is no silver bullet in what is best for everybody and their sales team tries to find the best fit for everybody within their budget and needs. If you have feedback that members have in something that they could build together, the PSCIOC endorses and categorize things, in certain stage of maturity, these Microsoft license SKUs could be beneficial for a security or privacy compliance and the MS team can explore this further.

Zelko Holjevac noted that the primary objective of the current discussion is to kick start the conversation. For Microsoft would be to understand some of the complexities that the jurisdictions are facing with the Microsoft products and services, because they are complex as they noted around licensing and that hasn't changed. Licensing is a sore point for jurisdictions. The conceptual idea of trying to get together and build synergies across the jurisdictions to see what they

can come up with. To ensure that Microsoft understands what members are trying to do and then take offline and have a series of discussions and workshops with Microsoft O365 WG and IT Procurement Community of Practice to figure out on how they build something that they jointly stand up as a Canadian jurisdictional SKU. Need to bring some outside of the box thinking. Members understand that Microsoft has rules and regulations and SKUs and a global product. Let's see how far we can push this along to try to make it as simple and easy for the Canadian jurisdictions as possible to move forward with the Microsoft tools and technologies.

John Hewie stated that Microsoft is always open for feedback. In the short term it would be more productive for them to explore some use case scenario, i.e. information classification and labeling. For jurisdictions as example labeling, what is built in Ontario was a great design pattern which has different encryption levels on who owns the key and who doesn't for different classifications. That is a use pattern or design pattern that is more applicable to a broad number of jurisdictions. Let's document aspects of that and talk about licensing pieces that are required to enable that.

Zelko Holjevac added that Information Management has been a discussion topic with the working group and it is an area that they could look into.

Members' Comments:

- It was stated that small communities in the north particularly Indigenous government organizations, they don't have the scale, depth and expertise to engage in fully as large jurisdictions can such as Ontario or British Columbia. They have the shared obligation as the CIO to the public sector to try and ensure that they are building up a framework that supports all levels of governments and they can ensure their responsibilities for information integrity and assuring the security and privacy, recognizing that many of these small jurisdictions do not have the staff, the knowledge and expertise and in many cases even the financial resources to do it on their own and they need to work with companies like Microsoft to achieve that.

John Hewie responded that Microsoft is committed to doing what is in the realm of the possible for them. Having a pan-Canadian agreement that multiple jurisdictions can procure from isn't possible in the way the things are structured today. There are different account teams that support individual jurisdictions, they continue to negotiate based on several criteria, size, other negotiation types of leaders. They offer very favorable prices to public sector that is resilient. In terms of helping to develop artifacts that can scale or design patterns or use case scenario and working with Microsoft team to document those for the Canadian context to meet Canadian privacy legislation or security privacy requirements, they are happy to engage in this. John Weigelt is leading the landing page built the service trust portal on the Microsoft site that is specific to Canada, that is the place where they publish their audit reports, members can verify that they are doing the things that they are saying they are doing on the security and privacy topics. John Weigelt recognized that jurisdictions are doing PIA (Privacy Impact Assessment) work. Early PIA work on the Cloud and they've seen a lot of duplication of efforts. In consultation with privacy experts across jurisdictions, John Weigelt led the development of those foundational PIAs. BC and ON have used them in the past and Microsoft updated them this year to include Teams which was a big ask and with the changes with the BC privacy legislation. They are happy to continue to do that and publish the work there or some other place that has meaningful value for members and better scales and learning and reduce duplication of efforts.

John Weigelt reiterated and following the conversation from last year, they put aside a budget ask to put a portal together for the public sector CIO Council for shareable artifacts, they are committed to the idea of scale, if they build for one jurisdiction, they can have reusable components across other jurisdictions. Unfortunately, due to COVID,

they didn't get traction on that GitHub location, but they continued to drive that forward and hope to use Microsoft Technology Centre in the Ottawa office for public sector use cases. The PSCIOC would be instrumental in helping Microsoft of what some of the use cases are because they cannot build them on their own. They need to learn what are members critical needs and work in collaboration with government partners to make those reusable components.

- What is needed based on listening to various jurisdictions with some of the common requirements and challenges that they all face and trying to help themselves down the road as they are going through the existing contracts and as they are also looking through, re-contracting and re-procurement as their contracts are expiring and for the new jurisdictions coming on board, is how they pull out that information together to make it as seamless as possible. They are trying to do things simpler for everybody to be able to consume. The group still has work to do in terms of products that jurisdictions may need as part of the general SKU, but if they get everybody to start from somewhere, not from zero, that would be success, how to come up with a plan to move forward and help everybody out.

John Hewie responded that he has been invited over the years to participate in PSCIOC's NCSIP meetings with CISOs across the country. He is open to participating in meetings of the Microsoft Office 365 Working Group or whatever structure Zelko puts in place and Microsoft will provide the right person to participate and drive that forward to meet those expectations from CIO members.

John Weigelt added that there are pockets of modern workplace user groups or MO365 user groups and they can provide visibility on when that is happening, all are now gone virtual and they can record and share those examples.

- John Hewie commented that he will give some of the examples that they are working on to improve the MS O365 experience and scale, which should be available soon. The compliance score in the platform is the evolution of compliance manager in the process of building up the protected B level in partnership with Po-Tea Duncan at TBS and the Canadian Centre for Cyber Security. It is based on CCCS medium security control profile. There is an opportunity for different jurisdictions to create their own templates. Microsoft recommends jurisdictions to improve security posture of their tenants. Compliance score leverages not only technical control but also the process, operations and compliance control, especially if members need to demonstrate compliance to their internal audit teams or other requests. This will help shape, help and guide people at the working level to make sure those configurations are set up and maintained. You have a set of KPI: secure score KPI, compliance score KPI. They can use the government-based line as a starting point and enable that for jurisdictions and members could manage in the future, there is lot of opportunity there to explore going forward.

John Weigelt added that there were recent announcements about the partnership with Academic institutions across Canada around skilling and re-skilling activities and efforts and there is an emphasis on public sector across communities around availability of course material and skilling those efforts. They done some work with the Government of Québec around skills development on Cloud, AI skills, and data skills but within a community like PSCIOC that represent broad jurisdictions across Canada this might be an opportunity to explore further.

Discussion on the Canada-specific Online Services Agreement (OSA) and Data Protection Addendum (DPA) that covers several of members unique concerns, for example, how Microsoft deals with law enforcement requests from the US Government relative to the Cloud Act:

- John Hewie stated that they did an internal refresh for internal teams on how they handle government access to request for data, with numerous questions about the Patriot Act and what is the risk, what is the Cloud Act, and what

does that mean? They have an intention to work bilaterally with governments and do a bilateral agreement but that is not in place yet. What are the real numbers, what are the requests? The fact that the numbers are small, and they have never provided content to a government request for public sector agency ever in the history of their Cloud operations globally, these are important things for people to understand.

- It was suggested that the high-level overview would be appreciated because it was raised by the community in the working group and then the working group could get into more details if needed.
- Cory Freed noted that many members are familiar of the Microsoft approach to law enforcement, as there were discussions on that over the years between members and Microsoft. Microsoft wasn't shy in this area in terms of challenging foreign law enforcement requests. Thinking about that issue at a high level and Microsoft holistic approach to how they balanced public safety but also online security he broke it down to three buckets:
 1. Bringing legal challenges to reinforce protection for their customers;
 2. Advocating a policy change and reform of data laws and
 3. From a contractual perspective, is being transparent with their customer and provide commitments that they need and information they need to understand the practical risk versus the theoretical risk.

Microsoft hasn't been shy challenging the US Government related to the Warrant Case that they took up to the Supreme Court. What came from that was the enactment of the Cloud Act. The Cloud Act is a piece of legislation in the US which creates a framework for the modern era, and they hope that is a potential for a lasting solution for the conflict of law issue around data sovereignty. The Cloud Act stands for great work that Microsoft did in terms of challenging the Government. The Cloud Act provides service providers like Microsoft with lots of protections that they are looking for to help protect their customers. One of the most important things is that it gives the country the ability to enter bilateral agreements with the US that basically dictate on how they co-operate and share information and also balance investigative requests for digital evidence. Canada does not have a bilateral agreement with the US yet, but the Cloud Act reinforces a lot of the protection that we rely on that challenges the US Government giving us the right to challenge the commodity concerns that might come up in case of a conflict and allows us to be transparent.

Microsoft doesn't provide any government with direct access of data. Data is owned by customers, not by Microsoft to the extent that they ever get a request from someone, they direct it to the customer. If you look at the data protection terms for online services, it is a standard provision that Microsoft provides to their customer around challenging these requests. They comply with the applicable law, to the extent that they ever get a request it has to follow the legal process, it has to be a warrant or order related to a criminal investigation. In the event that they ever respond to a request is for a specific account or identifier, it is never for an organization or a group of individuals. Most important how to describe, the practical risk versus theoretical risk. The theoretical they can tell you in contractual agreement that they never respond to a request from the US government, they cannot do that, because they are abiding the law. From a practical perspective, it is impossible to happen. They published the number of legal demands that they get every year. They do that twice a year: at the beginning and end of the year, when they disclose the number of requests that they receive and what was disclosed. They have never received a request from a public sector customer in Canada or they made the decision not to publish that. With the protection they have in the Cloud Act they have a very good story to tell and that would provide a lot of assurance to customers. When they think about theoretical risk versus practical risk, ultimately what Microsoft wants to leave customers with is: if data sovereignty is what concerns you the most, you are thinking about the wrong things.

	<ul style="list-style-type: none"> • Pleased to hear that Microsoft is willing to come to the table and to work with Microsoft Office 365 Working Group to discuss all these aspects in depth – that is a key deliverable that members wanted accomplished at the current PSCIOC meeting. • Pleased to hear that the O365 WG will have an in-depth discussion with Microsoft on the practical concerns as opposed to theoretical concerns. She wanted to ensure that all these concerns are raised. • John Hewie thanked PSCIOC members and responded that for Office 365 there is more in the truck in terms of capabilities and they lean on their account teams to help do that education across CIO members' teams. Microsoft will keep members abreast of the rapid pace of innovation and full transparency and even for them is sometimes hard to keep up with the pace of the innovation. He encouraged Tracy Wood and Zelko Holjevac to reach out to him and his team and they will provide the right people to cover the topics that have been discussed in the meeting. <p><i>Microsoft team left the meeting.</i></p> <p>Debrief of session with PSCIOC members:</p> <ul style="list-style-type: none"> • Tracy Wood asked members if they were pleased with the discussion with Microsoft and where this landed. • It was stated that this was a much more positive discussion than at the previous meeting in 2018, however a bit disappointed that Microsoft is not going to come to a pan-Canadian agreement or a Canadian SKU. • It was noted that the main objective was for Microsoft to be willing to come to the table and have further discussion on specific issues; this was accomplished today. It is important that they are willing to participate in further discussion with the MS O365 Working Group. The MS O365 Chair will follow up with John Hewie on the items discussed above and report back to the PSCIOC members at a future meeting. • Tracy Wood thanked Zelko Holjevac and the MS O365 Working Group for all the work and effort to make this happen. 	
3	<p>NATIONAL CIO SUB-COMMITTEE ON INFORMATION PROTECTION (NCSIP) (Refer to TAB 3)</p> <p>Alexandra Underhill, Chair of the NCSIP, Canadian Centre for Cyber Security provided a presentation on best practices related to security incidents handling (reporting scams).</p> <p>She spoke about the Mandate of the Cyber Centre, RCMP, NC3, Canadian Anti-Fraud Centre, SPAM Reporting Centre and best practices on reporting scams. She advised that the new CSE Act came into force on August 1, 2019. The new legislation builds on CSE's previous mandate which was to:</p> <ul style="list-style-type: none"> • protect information and information infrastructures of importance to the Government of Canada; • collect foreign communications to produce foreign signals intelligence (SIGINT), in accordance with Government of Canada intelligence priorities. This supports government decision-making on matters of security, national defense and international affairs in accordance with those priorities; and • provide technical and operational assistance to federal law enforcement and security agencies in their legally authorized activities 	<p><i>No action item resulted from this discussion. NCSIP has a pending action item related to</i></p>

To ensure they kept up with technology and the changing security environment, while being able to offer our best support to Canadians, the new Act introduces a **few new authorities for CSE**:

- In addition to their current cyber security and information assurance mandate, they now have a new authority to defend important networks outside of the Government of Canada. This assistance could include, for example, deploying CSE's unique cyber security tools on non-Government of Canada systems.
- The CSE Act also explicitly allows CSE to share cyber threat information with owners of systems outside of the Government of Canada so that they can better protect their networks and information. For example, CSE could more extensively share information about specific cyber threats with the owners of critical infrastructure, like telecommunications companies or the finance sector.
- The CSE Act also gives CSE the ability to take action online, outside Canada, to defend important Canadian networks and proactively deter cyber threats before they reach important Canadian systems.

These new authorities, combined with the Cyber Centre, will better protect Canadians' most sensitive information and important cyber networks from compromise, strengthen Canada's cyber defenses, and ultimately make Canada the safest place to live and work online.

Members' discussion:

- Natasha Clarke stated that the current reporting structure is a lot to navigate through when you are in the middle of an incident. Has there been discussion on how they can have a user centric approach to this and have a centralized function? Can the Cyber Centre help to navigate this on behalf of the user? Has there been any discussion to simplify that from a user centric perspective?

Alex Underhill responded that the Canadian Centre for Cyber Security is currently working on a central platform. Working on a reporting mechanism that will guide members and jurisdictions to the right reporting agency. All agencies work on the same platform and if members report it to one of the agencies, then it will be directed to the right agency. She encouraged members to report security incidents to the Canadian Centre for Cyber Security, they have the guidance and expertise. The CCSC is not a vendor so they cannot provide actual support, but they can share information with other agencies and other sectors.

- Gary Perkins commented that there are so many incidents and jurisdictions are left with making a decision as to whether work on the incident or report it. This means that if they don't report it then this does not get tracked or accounted for. In recent years the RCMP on the west coast got very low reports in numbers and when it comes to Central to provide funding for them, they don't get any funding to grow their cyber program because of the low number of incidents reported. The longer this remain the case, the longer they remain limited in their ability to assist those affected. The decision when and why or why not to engage the law enforcement agencies is covered in the course. Members should report incidents as this is a matter of public record.
- Tracy Wood added that when they reported an incident, their legal team wanted to be there all the step of the way and her team wasn't necessarily available at the time. They were pleased to have RCMP involvement but legal teams want in on that conversation too, so this is something to keep in mind.

	<ul style="list-style-type: none"> Alex Underhill commented that at CCSC they have a nondisclosure agreement in place and private sector reports more to them than to law enforcement because they have that non-disclosure agreement. David Hayes stated that in his jurisdiction the OPP has a Cyber Crime Unit and if you report to local police in the jurisdiction, they need to bring that up to the OPP and in some of cases they are parachuting and give you a high level assistance. Keith Douglass inquired if for O365 clients, does using the Microsoft "report a spam / phish" button sent the message to all the correct agencies? <p>Gary Perkins responded that incidents like this are significantly underreported to law enforcement and other organizations. The problem with this is that these organizations don't get as much funding to assist in the future.</p>	
4.	<p>JURISDICTIONAL INFORMATION SHARING (TAB 4A to 4N)</p> <p>Jurisdictions provided a brief summary of their key priorities and activities in their respective jurisdictions. Members can refer to the jurisdictional information sharing documents provided in the meeting binder for details. (TABS 4A to 4N)</p> <p><i>Please note that as per current practice, due to the sensitive nature of this discussion only action items arising from jurisdictional information sharing roundtable are included in the Record of Decision.</i></p> <p><u>Jurisdictions that provided an update:</u></p> <ul style="list-style-type: none"> Treasury Board of Canada Secretariat Yukon Northwest Territories Nunavut Ontario Saskatchewan Manitoba Québec New Brunswick Nova Scotia Prince Edward Island Newfoundland and Labrador MISA 	<p>Action Item #3: Topics tabled for discussion at future PSCIOC meetings:</p> <ul style="list-style-type: none"> Digital signatures approvals Framework for decision-making for risk management and investment plan. E-service design Payment gateway HR policy for remote work Oracle RDBMS alternatives like PostgreSQL (PostgreSQL database is open-source and object-relational database management system whereas Oracle is a commercial relational database management system which is available in different editions.) Cost recovery model for infrastructure technology services IT investment and demand planning with funding related to capital pieces Chatbots Managing government data on citizens

		<ul style="list-style-type: none"> Implementation of network of cyber defense at government levels and management of information security
5.	<p>Other Business</p> <p>Tracy Wood and Denis Skinner thanked members, presenters, and observers for participating in the PSCIOC meeting. Tracy thanked the ICCS for organising and managing the virtual meetings. She noted that there is a lot of work behind the scenes to ensure that everything goes smoothly.</p> <p>Tracy encouraged members to complete the evaluation form at the end of the meeting. The evaluation form is available on MS Teams and the ICCS will email the link to all participants.</p> <p><i>The PSCIOC meeting adjourned at 3:10 p.m. EDT.</i></p>	