CANARIE Annual Business Plan

2025-26 (FY26)

March 19, 2025

canarie.ca | @canarie_inc

Table of Contents

1. Executive Summary

CANARIE is pleased to present its Annual Business Plan for fiscal year 2025-26 (FY26), the first year of its new 2025-30 mandate. The document includes CANARIE's plans to achieve its expected results in FY26, as well as CANARIE's risk position and the organization's risk mitigation strategies.

1.1 Role of CANARIE

Together with our 13 provincial and territorial partners, we form Canada's National Research and Education Network (NREN). This ultra-high-speed network connects Canada's researchers and educators to each other and to global data, technology, and colleagues.

To strengthen the security of Canada's research and education sector, we collaborate with our partners in the NREN, government, academia, and the private sector to fund, implement, and support cybersecurity initiatives. We also provide identity management services to the academic community through eduroam and identity and access management services.

Established in 1993, CANARIE is a non-profit corporation, with most of our funding provided by the Government of Canada.

1.2 Vision and Guiding Principles for the 2025-2030 Mandate

CANARIE's vision for our 2025-2030 mandate is "A more secure and innovative Canada."

In Network Operations, CANARIE's strategy is to evolve and expand the CANARIE Network in a flexible and cost-effective manner over the long-term, by deploying fibre from coast-to-coast across Canada. This provides the flexibility to add capacity and deploy transformative technologies quickly and at a considerably lower incremental cost, especially as network traffic is expected to continue its significant growth in the future. This connectivity is protected by leased services, which provide necessary network diversity and additional reach. CANARIE also supports access to the CANARIE Network by helping evolve Canada's federated National Research and Education Network (NREN) in a coordinated manner, and by providing Identity and Access Management services to ensure that researchers in Canada can safely and securely access data sets, infrastructures, and tools across the globe.

In Cybersecurity, CANARIE offers tools, services, and national coordination, to help improve the cybersecurity and resilience of the research and education communities in Canada, around the concept of Collective Cybersecurity. All CANARIE activities are focused around four core pillars to support this goal: (1) assessing and prioritizing community risk (for example, the National Cybersecurity Assessment; Benchmarking; etc.); (2) gathering, analyzing, and sharing actionable threat intelligence (for example, the Threat Feed, Dark Web Monitoring, etc.); (3) synchronizing triage and accelerating response to cyber incidents (for example, the CanSSOC Federated SOC Pilot); and (4) pooling and sharing resources (for example, common templates, frameworks, content, etc.).

1.2 Focus of Activities: FY26 (April 1, 2025 to March 31, 2026)

In addition to the ongoing management and evolution of the CANARIE Network and other programs, CANARIE's key planned activities and outcomes in FY26 to help support our mandate vision for "A more secure and innovative Canada" include:

- Continued work on the 400Gbps capacity upgrade of the CANARIE Network
- Complete data collection on the CanSSOC Federated SOC Pilot and deliver funding request to ISED
- Continue to evolve and optimize the Cybersecurity Initiatives Program (CIP) aligned to outcomes across the four strategic pillars
- Evolve the National Cybersecurity Assessment service and create greater alignment with other sector-wide assessment and risk prioritization initiatives
- Work with the community to share the outcomes of the March 2025 Cybersecurity Visioning and Strategic Alignment Workshop and the findings of the cybersecurity Investment Analysis and Blueprint projects
- Expand the portfolio of identity-based services, focusing on offering Federated Identity Management as a managed service deployment
- Launch NREN Call 1 to enable the NREN to create, extend, or improve network and security infrastructure and to develop and retain talent; and
- Engage in ongoing coordination with the Digital Research Alliance of Canada (the Alliance) in support of the Government of Canada's Digital Research Infrastructure Strategy.

2. 2024-25 Accomplishments to Date

2024-25 (FY25) is the fifth and final year of CANARIE's 2020-2025 mandate. The following sections provide an overview of CANARIE's accomplishments in FY25 to date, under each of the three Eligible Activities outlined in the 2020-2025 Contribution Agreement that govern the mandate, along with information on outstanding projects for completion. Thus far in FY25, CANARIE:

- Deployed equipment to additional segments of the CANARIE Network in support of upcoming 400Gbps capacities
- Renewed CANARIE's Indefeasible Right of Use for 20 years on the eastern optical fibre path
- Continued to roll out *eduroam* wi-fi access authentication through service providers in public, non-institutional environments such as airports and libraries
- Launched the third round of the National Cybersecurity Assessment (NCA) service
- Continued to execute the CanSSOC Federated SOC Pilot
- Evolved the national Threat Intelligence service with addition of dark web monitoring, continued expansion of community engagement, and integration into the CanSSOC Federated SOC Pilot
- Launched the cybersecurity Investment Analysis and Blueprint projects to understand (1) the sector's current cybersecurity investment landscape, and (2) the essential components and best practices needed for a secure research and/or education organization in Canada
- Hosted the 2024 NREN Assembly to strengthen collaboration among the Canadian NREN Partners
- Hosted the 2024 CANARIE Summit, focused on "Transformative Innovation for Good"
- Hosted the inaugural standalone Canadian SecuR&E Forum, a community focused cybersecurity event for the community
- Prepared for the 2025-2030 Mandate by aligning the organization to support mandate delivery and communicated elements of CANARIE's next Mandate to the community; and
- Advanced international cybersecurity initiatives.

Key projects to be completed or kicked off before the end of FY25 include:

- Bringing together the community for a Cybersecurity Visioning and Strategic Alignment Workshop.

The balance of FY25 accomplishments will be captured in the Annual Report.

3. 2025-26 Planned Activities

FY26 will be the first year of CANARIE's new 2025-2030 mandate. To deliver on its expected results for the mandate, CANARIE will undertake the following activities in the 2025-26 fiscal year:

3.1 Network Operations

CANARIE will continue to undertake all required activities to support and evolve the existing CANARIE Network and the services delivered over it.

3.1.1 Network Program

In FY26, the CANARIE Network will continue to operate and evolve as essential research infrastructure to support research, education, and innovation:

FY26 Activities	FY26 Short- and Medium-Term Outcomes
Operate the Network Increase capacity, redundancy, and reliability Continue to improve the Network's security posture Improve network monitoring activities through the adoption of new tools Continue to enhance user access to support tools Continue to develop network service automation Operate the Distributed Denial of Service (DDoS) detection system dedicated to the CANARIE Network Develop strategies for leveraging AI to improve the efficiency, reliability, and security of network operation Safeguard the Network and CANARIE by implementing measures to prevent, detect, and respond to cyber threats, ensuring the integrity, confidentiality, and availability of data and systems Engage on international networking activities, including polar connectivity and GNA-G (Global Network Advancement Group)	Deployment of additional network capacity to support traffic growth Improved access to commercial cloud services Continued work on the 400Gbps capacity upgrade Completion of the refresh of the Eastern fibre systems Improvement of the network security reporting, monitoring, and measurement system Deployment of Network Automation Applications and continued work on the Automation development Developed plans for leveraging AI in network operation Deployment of support tools accessible through the user portal

3.1.2 Infrastructure Extension Program (IEP)

In FY26, CANARIE will support government research institutes leveraging the research network in support of collaborative research with national and international partners, with the aim of moving these final connections to Shared Services Canada (SSC) by the end of FY28:

FY26 Activities	FY26 Short- and Medium-Term Outcomes
Provide existing high-speed network connections to government research facilities Ensure connections are adequate to meet user needs Planning to transition existing IEP connections to SSC	Continue to support existing connections to government research facilities that meet the performance needs of the government science community

3.1.3 Identity and Access Management

In FY26, CANARIE will provide robust identity and access management services that enable secure and efficient remote access to distributed resources and tools, anytime, through the Canadian Access Federation (CAF) Program:

FY26 Activities	FY26 Short- and Medium-Term Outcomes
Continue to work with Canadian Access Federation (CAF) participants and industry experts to plan how CAF can evolve Expand the number of sites that broadcast eduroam in the community to offer options for distance learning and creative utilization of community spaces Expand the portfolio of identity-based services, focusing on offering Federated Identity Management as a managed service deployment Engage with the international community on the evolution of identity management services	Maintain the current high level of participation in CAF Increased number of eduroam log-ins per year Increased number of projects to upgrade the capacity/capability of the Federation Increased number of interfaces, applications, and tools available to support CAF services

3.1.4 NREN Program

In FY26, CANARIE will support the continued evolution of the NREN such that it acts in a coordinated manner to advance common objectives, while respecting and leveraging the diversity within the federated model:

FY26 Activities	FY26 Short- and Medium-Term Outcomes
Extend capacity, redundancy, reliability, and security through provincial and territorial NREN Partners' networks Connect research and education facilities including in the North Strengthen the cybersecurity of the NREN Further enhance the processes and capacity of the NREN and support and retain talent	Execution underway to launch Call 1 to enable the NREN to create, extend, or improve network and security infrastructure and to develop and retain talent Development and launch of projects to enhance the processes and capacity of the NREN Scoping work underway to launch Call 2 in FY27 to connect the unconnected including indigenous institutions to the NREN

3.2 Cybersecurity

In FY26, CANARIE will work to support the improvement of the overall cybersecurity posture of the research and education sector:

FY26 Activities	FY26 Short- and Medium-Term Outcomes
Complete the CanSSOC Federated SOC pilot, evaluating its impact, outcomes, and lessons learned, and evaluate options for continued service Expand Threat Intelligence service, including the integration of the Threat Feed with the CanSSOC Federated SOC Pilot to enhance threat intelligence and proactive defense Explore an information-sharing platform to support the exchange of templates, frameworks, and ideas across the sector Develop shared frameworks, policies, templates, and collaboration tools to improve consistency and alignment within the community Identify and deliver cybersecurity initiatives informed by data and analysis for broad sectoral benefit Launch targeted marketing to increase awareness and engagement with CANARIE cybersecurity initiatives among eligible organizations Enhance community engagement with agile, informal channels to complement existing advisory structures, to advance sector-wide cybersecurity capabilities Strengthen collaboration with Canadian cybersecurity organizations to benefit the R&E sector and the broader economy Refine and expand high-value initiatives based on insights from past pilots and projects	Deploy and refine initiatives under the four strategic cybersecurity pillars: Community Risk Assessment; Threat Intel; Cyber Response; and Pooling and Sharing Resources Complete data collection on the CanSSOC Federated SOC Pilot and deliver funding request to ISED Expand the CanSSOC Threat Feed into a comprehensive national Threat Intelligence service Host events and provide thought leadership to enhance engagement and alignment with the community Evolve the National Cybersecurity Assessment service and create greater alignment with other sector-wide assessment and prioritization initiatives Establish a robust framework for ongoing community engagement and collaboration, including clarity of roles and responsibilities

3.3 Activities in concert with the Digital Research Alliance of Canada

In FY26, CANARIE will work with the Digital Research Alliance of Canada (DRAC) to support the Government of Canada's Digital Research Infrastructure Strategy:

FY26 Activities	FY26 Short- and Medium-Term Outcomes
Work to integrate CANARIE and DRAC tools and services, including in cybersecurity Ongoing alignment of governance, communications, and outreach activities Discussions to support Government of Canada science, including science-based departments and agencies, as well as Government of Canada science policies	DRAC and host sites participating in the National Cybersecurity Assessment Ongoing planning for common cybersecurity approaches, including activities where the Alliance's cybersecurity activities feed into and benefit from the CanSSOC Federated SOC approach Alignment on cybersecurity governance for the two organizations, including a single individual chairing both organizations' cybersecurity committees Continued work to integrate Federated Identity Management into the Alliance's ARC services CANARIE participation in cloud pilot project processes

3.4 Activities Supporting Equity, Diversity, and Inclusion

In FY26, CANARIE will work to advance Equity, Diversity, and Inclusion (EDI), both internally and in the programs we deliver:

FY26 Activities	FY26 Short- and Medium-Term Outcomes
Work in Canada and internationally to support underserved communities Training for CANARIE staff on topics that advance EDI Continued work to renew CANARIE policies, procedures, and practices Ongoing Indigenous community engagement strategy and activities Work with partners in the DRI ecosystem to coordinate joint policy positions on EDI Continued use of institutional EDI plans as an adjudication criterion for funding selection, where appropriate	Scoping work underway to launch NREN Call 2 in FY27 to connect the unconnected including indigenous institutions to the NREN Continued engagement with submarine Arctic cable consortia to support Northern Connectivity Ongoing support for CANARIE Employee Resource Groups Deliver additional training for staff as appropriate

4. Program Delivery Timelines

		Fiscal year 2025-26			
Eligible Activities	**Initiatives**	**Ongoing**	**Projected or *Actual* Launch**	**Major Milestones (Previous)**	**Projected Completion (Previous)**
Network Operations					
Network Program	Operate the Network				
	Increase capacity, redundancy, reliability - Milestone 6: Eastern fibre optical equipment install - Milestone 7: 400Gbps services launched on eastern network, complestes 400Gbps capabilities west and south of Montreal - Milestone 8: Removal, cleanup complete of old equipment		***2020-04-01***	**2025-08-22** **2025-09-26** **2025-11-28**	**2025-11-28**
	Continue to enhance network security and measurement monitoring tools				
	Continue to develop software-driven network services - Milestone 1a: Software driven network platform demonstration - Milestone 2: Platform aware of network inventory - Milestone 3: Platform initiated network configuration demonstration		***2023-04-01***	**2025-05-30** **2025-09-26** **2026-02-26**	**2030-03-31**
	Upgrade of the Distributed Denial of Service (DDoS) detection system of the CANARIE network - Milestone 1: Selection of vendor for equipment, services - Milestone 2: New DDoS system in operation - Milestone 3: Tuning complete, in production		**2025-04-01**	**2025-08-29** **2025-11-28** **2026-02-27**	**2026-02-27**
	Cybersecurity monitoring on CANARIE infrastructure, services and network, NREN Partners self monitor for cybersecurity.				
	Operate the Distributed Denial of Service (DDoS) detection system dedicated to the CANARIE network and actively collaborate with NREN Partners				
	Promote and implement in-house cybersecurity expertise development for CANARIE dedicated security staff and NREN security analyst community				
IEP Program	Provide high-speed network connections to government research facilities - Milestone 1: Plan for SSC to take over existing CANARIE connections		**2025-04-01**	**2025-06-27**	**2027-03-31**

Eligible Activities	Initiatives	Ongoing	Projected or *Actual* Launch	Major Milestones (Previous)	Projected Completion (Previous)
Identity and Access Management Program	Promote the adoption of the eduroam Configuration Assistant Tool (CAT) profile to elevate the security posture of the entire eduroam community				
	Development of more robust technical documentation and tutorials to simplify deployment, operation, and use of eduroam and IAM services				
	Promote managed service technology that make eduroam easier to deploy, to expand the number of sites that broadcast eduroam wifi in the community				
	As with using managed service technology for eduroam, do similar for identity access management in the community - Milestone 1: Managed service technology chosen - Milestone 2: Pilot service with test institutions - Milestone 3: Managed service technology ready for wider deployment		**2024-08-07**	**2025-01-30** **2025-04-03** **2025-08-22**	**2025-09-26**
	Identity access management community needs assessment - Milestone 1: Market research vendor chosen - Milestone 2: Draft results available - Milestone 3: Translation into elements of an IAM community of practice plus tailoring of CANARIE program delivery		**2025-03-04**	**2025-06-27** **2025-12-12** **2026-02-27**	**2026-03-27**
NREN Program	NREN Call 1 - Milestone 1: Call charter approved - Milestone 2: Launch of call to NREN Partners - Milestone 3: Selection of projects		**2025-01-13**	**2025-01-30** **2025-04-03** **2025-10-08**	**2028-01-31**
	NREN Call 2 Connecting Unconnected - Milestone 1: Call charter approved		**2025-07-01**	**2025-12-12**	**2029-01-31**

Eligible Activities	Initiatives	Ongoing	Projected or *Actual* Launch	Major Milestones (Previous)	Projected Completion (Previous)
Cybersecurity	DNS Firewall, Threat Feed, National Cybersecurity Assessment, Benchmarking initiatives continued operations for all interested eligible organizations.				
	CanSSOC Pilot - Milestone 3 : Data collection complete - Milestone 4: Funding request delivered to ISED		***2023-09-03***	**2025-06-30** **2025-09-12**	**2026-08-28**
	IS Assessment data collection platform improvements - Milestone 1: Select vendor - Milestone 2: Improvements complete for launch of 4th year assessments		**2025-04-01**	**2025-07-25** **2025-10-31**	**2026-03-31**
	CanSSOC shared security operations centre				
	CanSSOC Threat Feed evolution - Milestone 1 : Duplicate McGill hosted threat feed at CANARIE - Milestone 2: Improvements implemented, daily operations transferred from McGill to CANARIE		**2025-04-01**	**2025-09-26** **2026-02-20**	**2026-03-31**
Activities in concert with the Digital Research Alliance of Canada					
Cybersecurity	Alliance and Host Sites use National Cybersecurity Assessment (NCA) - Milestone 1: Decision on administrator of NCA questions for Host Sites - Milestone 2: NCA assessment registration		**2025-04-01**	**2025-07-31** **2025-09-30**	**2026-02-27**
	Alignment on cybersecurity governance for the two organizations, including a single individual chairing both organizations' cybersecurity committees				
	Continued work to integrate Federated Identity Management into the Alliance's ARC services				
Activities Supporting Equity, Diversity, and Inclusion					
EDI	NREN Call 2 to connected the unconnected including indigenous institutions to the NREN		See NREN Call 2	See NREN Call 2	See NREN Call 2
	Continued engagement with submarine Arctic cable consortia to support Northern Connectivity				
	Ongoing support for CANARIE Employee Resource Groups				
	Deliver Additional training for staff				

5. Representation and Financial Plan

The Government of Canada is investing $176M to support CANARIE's activities from FY26-FY30. This funding commitment ensures that CANARIE can continue to deliver strategic investments in infrastructure and services for Canada's research and innovation communities. As per the Contribution Agreement, $29,600,000 is allocated for FY26 activities, CANARIE covenants and agrees to hold, invest, administer, and disburse that amount in accordance with the stipulations of the Contribution Agreement.

5.1 Program Revenues and Expenditures

The following table summarizes CANARIE's program revenue and expenditures budget for FY26:

	(in 000s)
Revenues	
Funding	
Government of Canada	29,600
Total Funding	**29,600**
Program Revenues	
User Fees	650
Interest Income	50
Total Program Revenues	**700**
Total Revenues	**30,300**
Expenditures	
Program Expenditures	
Network Operations	
Network Infrastructure & Services	15,517
NREN	973
CAF	1,928
Total Network Operations	**18,418**
Cybersecurity	
Cybersecurity Programs and Services	5,041
CanSSOC Federated SOC Pilot	1,623
Total Cybersecurity	**6,664**
Total Program Expenditures	**25,082**
Administration Expenditures	5,218
Total Expenditures	**30,300**
Excess of Revenues over Expenditures	-

5.2 Funding Requirements

As indicated in the Program Revenues and Expenses shown above, CANARIE's cash requirement for FY26 is $29.6M.

5.3 Representation

CANARIE represents that it is not in default under the terms of the Contribution Agreement that is currently in force.

5.4 Cost Recovery

The following table summarizes CANARIE's cost recovery projections for FY26.

	FY26 (in 000s)
Cash	
IEP User Fees - Federal	100
IEP User Fees - Non-federal	6
Participant Fees	544
Total Cash	**650**
Matching Funds	
NREN	*0*
Total Matching Funds	**0**
TOTAL COST RECOVERY	**650**

Throughout FY26, CANARIE will continue to charge fees to users of CANARIE services and programs.

- As part of the legacy infrastructure extension program (IEP), CANARIE supports the costs to connect federal and non-federal labs to the NREN. The federal IEP connections' cost recovery is a fixed annual amount paid by Shared Services Canada to offset the total annual cost of supporting these connections. For non-federal IEP connections, the amount in the budget represents 100% cost recovery of planned expenditures.
- Participant Fees include cost recovery for the CAF program and other Network program initiatives.
- The NREN program will result in sharing of costs between CANARIE and other funding sources (e.g., provincial government, NREN partner funds, etc.) for funded projects. CANARIE's contribution level will be determined on a project-by-project basis. CANARIE will ensure the outcome of the NREN program meets its overall cost recovery target, hence, greater priority will

be given to projects which have leveraged contributions. However, because claims for NREN Call 1 are not expected until FY27, the cost matching for FY26 is projected to be nil.

5.5 Investment Policy and Strategy

CANARIE shall continue to invest and manage any advanced funds according to investment policies, standards, and procedures that a prudent person would follow in making investment decisions regarding property belonging to others. CANARIE will manage the funds in accordance with the Contribution Agreement and, the investment directives contained in Schedule E of the Contribution Agreement. The objectives are twofold: (a) to provide funds on an "as needed" basis to meet the disbursement needs of CANARIE and (b) to maximize the investment income earned by CANARIE, subject to the Investment Policy and Investment Strategy adopted by CANARIE. Investment decisions shall be made with the principal objective being the preservation of capital to meet future disbursement requirements.

The Investment Policy and the Investment Strategy specify permitted transactions and risk limitations for all market and credit risks faced by CANARIE, and levels of authority of officials who can commit CANARIE to different types of transactions. The Investment Policy and Investment Strategy must be reviewed annually: they were most recently reviewed and approved by the Audit and Investment Committee in October 2024. The Investment Policy is guided by the constraints contained in the Contribution Agreement.

6. Performance Monitoring Strategies, Risk Assessment, and Mitigation Strategies

6.1 Performance Monitoring Strategies

CANARIE collects metrics internally for all its programs, services, and for the network. External performance metrics are collected from the community in the form of user surveys, reports, and reporting from the regional networks. CANARIE works with the Minister to integrate this information as part of an overall performance management strategy. Additionally, performance data for each eligible activity is part of CANARIE's annual reporting.

6.2 Program Delivery Risks

Due to the diversity and complexity of the ecosystem CANARIE operates in, risk management is essential for CANARIE to achieve the expected results defined in the Contribution Agreement. Risk is reported on by Management and monitored by the Board of Directors.

Identified risks are classified based on the likelihood of occurrence of the risk, as well as the severity of the negative impact of the risk. The treatment of identified risks will vary based on these two dimensions as per the table below:

		Probability		
		Low	**Medium**	**High**
Impact	**Low**	Accept risks	Accept risks with monitoring	Monitor and manage risks
	Medium	Accept risks with monitoring	Develop formal risk mitigation measures	Develop formal risk mitigation plan
	High	Identify mitigation steps and monitor regularly	Develop formal risk mitigation measures and monitor regularly	Develop formal risk mitigation plan and monitor regularly

Please see Table below:

Risk Name	Description	Prob.	Impact	Risk	Mitigation Strategies and Action Plans
New Contribution Agreement Language	New Contribution Agreement contains new language and requirements which CANARIE will have to operationalize	H	M	HM	• Working with ISED to support their requirements
Supplier Risk	Supplier cybersecurity risk – supply chain risk	M	H	MH	• Include requirements in our procurement process that drive the management of cybersecurity risks • Legal language requirements under investigation • Supplier Code of Conduct developed. Working with Finance to evolve procurement practices • Risk related to sole source under investigation
Corporate IT Breach or subjected to Cybercrime	A breach of CANARIE's backbone network could expose research data, provide an attack vector on connected institutions, and pose reputational risk to CANARIE	M	H	MH	• Ongoing IT investments • Patching and upgrade practices • DDoS detection • Security awareness training, security monitoring • Cyber insurance • Incident response plans • First tabletop exercise run on March 2023 • Corporate tabletop exercise completed in November 2024. Business Continuity Plan and Incident Response Plan are being updated to reflect insights gathered from tabletop exercise. • Tabletop exercise with GREN partners held July 2024 • Regular security awareness briefings at monthly all-staff meetings
CANARIE Network Breach	A breach of CANARIE's backbone network could expose research data, provide an attack vector on connected institutions, and pose reputational risk to CANARIE	M	H	MH	• Security investments (e.g. SIEM) • DDoS Detection • MANRS Network Security Norms implemented
NREN Network Breach	A breach of an NREN Partner could, in turn, affect the CANARIE network, and pose a reputational risk to the NREN, and therefore CANARIE	M	H	MH	• Joint security investments (e.g. SIEM). • Security analysts are in place at NREN Partners and working together nationally. • Cybersecurity Framework adoption • NREN security scorecard implementation • Support NREN inclusion into the security operation centre (SOC)

Risk Name	Description	Prob.	Impact	Risk	Mitigation Strategies and Action Plans
					• MANRS Network Security Norms implemented across the majority of the NREN • Tabletop exercise held at NREN Assembly in October 2024
Risks of economic conflict (tariff war) between Canada and USA	If the US government implements tariffs on a broad range of Canadian goods and the Canadian Government reciprocates in kind, CANARIE may face difficulties purchasing or renewing contracts with American suppliers, impacting our operations	M	H	MH	• No ability to impact the risk • Watching brief
CanSSOC Federated SOC Pilot	Risk that the federated model and the inherent challenge of obtaining alignment from various stakeholders will lead to insufficient participation in the Pilot, which could limit the data available for analysis	L	H	LH	• HR working group • Information Security Leaders working group • Management oversight • NREN Partner engagement guiding principles adopted • Cybersecurity Advisory Committee endorsed CanSSOC Federated SOC Pilot Charter • Multiple information sessions hosted for participating institutions regarding content and form of information sharing agreements • Ongoing engagement with prospective participating institutions to facilitate and encourage onboarding • 13 institutions across 5 provinces have signed the agreement to participate in the Pilot
Joint Alliance Activities	Ongoing Contribution Agreement requirements that have dependency on the Alliance's ability to support the joint work required	L	L	LL	• Working with ISED, the Alliance, and the community to support the new organization • Meetings are on-going with the Alliance. Relationships with the President and other key staff at the Alliance continue to develop