CANARIE Annual Business Plan

2026-27 (FY27)

January 30, 2026

canarie.ca

Table of Contents

1. Executive Summary

CANARIE is pleased to present its Annual Business Plan for fiscal year 2026-27 (FY27), the second year of its 2025-30 mandate. The document includes the organization's plans to achieve its expected results in FY27, as well as its risk position and 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-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 augmented by evolving technologies such as Low Earth Orbit Satellites and leased connectivity 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 (IAM) services to ensure that Canada's researchers can safely and securely access data sets, infrastructures, and tools across the globe.

In Cybersecurity, CANARIE offers tools, services, and national coordination, to strengthen the cyber defences and resilience of the research and education communities in Canada, through the goal of "collective cybersecurity".

CANARIE's cybersecurity activities are focused around five core pillars to support this goal:

(1) Assessing and prioritizing community risk (for example, through National Cybersecurity Assessment; Benchmarking; etc.);

(2) Gathering, analyzing, and sharing actionable threat intelligence (for example, through Threat Feed, Dark Web Monitoring, etc.);

(3) Synchronizing, triaging and accelerating response to cyber incidents (for example, through CanSSOC Federated SOC, the Pilot of which has been completed and is awaiting full program funding from the Government of Canada);

(4) Pooling and sharing resources (for example, through common templates, frameworks, content, etc.); and

(5) Community engagement.

1.3 Focus of Activities: FY27 (April 1, 2026 to March 31, 2027)

In addition to the ongoing management and evolution of the CANARIE Network and other programs, CANARIE's key planned activities and outcomes in FY27 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
- Deployment of direct Asia Pacific connectivity to support global research activities
- Launch of NREN Program Call 2 to connect the unconnected, with a focus on Indigenous institutions
- Expand the portfolio of identity-based services, focusing on offering Federated Identity Management as a managed service deployment
- Continue to evolve and optimize the Cybersecurity Initiatives Program (CIP) aligned to outcomes across the five strategic pillars
- Engage in ongoing coordination with the Digital Research Alliance of Canada in support of the Government of Canada's Digital Research Infrastructure Strategy

2. 2025-26 Accomplishments to Date

2025-26 (FY26) is the first year of CANARIE's 2025-2030 mandate. The following sections provide an overview of CANARIE's accomplishments in FY26 to date, under each of the two Eligible Activities outlined in the 2025-2030 Contribution Agreement that govern the mandate, along with information on outstanding projects for completion. Thus far in FY26, major accomplishments include:

- Provided a national federated situational awareness model through the successful CanSSOC Federated Security Operations Centre Pilot.
- Submitted a proposal to the Government of Canada to fund the CanSSOC Federated Security Operations Centre as a core CANARIE service starting on April 1, 2026

- Upgraded the network optical equipment on the Winnipeg-Thunder Bay-Sudbury corridor, to support the connectivity needs of the research and education (R&E) community
- Hosted the 2025 SecuR&E Forum, to build community and foster learning and knowledge-sharing by connecting contributors to cybersecurity across Canada's R&E sector
- Selected and approved the projects to be funded under NREN Call 1, to enable the NREN to create, extend, or improve network and security infrastructure and to develop and retain talent
- Released the Cybersecurity Investment Analysis & Blueprint documents to the community, to build a national baseline of cybersecurity investment in Canada's R&E sector, and to understand where to invest more and find further efficiencies
- Implemented eduroam Service-Provider-as-a-Service as a key function of eduroam, to support the roll-out of eduroam in non-R&E locations
- Launched a monthly threat intelligence technical cybersecurity update for institutional security teams

Key projects to be completed or kicked off before the end of FY26 include:

- Completing the replacement of the hardware at MOXY, CANARIE's global exchange point in Montreal, in line with updating the capacity for the transatlantic connectivity to 400G
- Launching an annual executive cybersecurity briefing, to inform proactive defence, strategic planning, and budget decisions at institutions
- Launching the cybersecurity Community Collaboration Hub, to support the pooling and sharing of resources across the Canadian R&E sector

The balance of FY26 accomplishments will be captured in the FY26 Annual Report, to be provided to ISED in July 2026.

3. 2026-27 Planned Activities

FY27 will be the second year of CANARIE's 2025-2030 mandate. To deliver on its expected results for the mandate, CANARIE will undertake the following activities in the 2026-27 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 FY27, the CANARIE Network will continue to operate and evolve as essential research infrastructure to support research, education, and innovation:

FY27 Activities	FY27 Short- and Medium-Term Outcomes
▪ Operate the Network ▪ Increase capacity, redundancy, and reliability ▪ Improve network monitoring activities through the adoption of new tools	▪ Deployment of additional network capacity to support traffic growth, including increases to 400Gbps capacities cross the country, and increasing to 100Gbps services in Atlantic region ▪ Increased northern network capacity
▪ 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 ▪ Continue to improve the Network's security posture ▪ Refresh the end-of-life Distributed Denial of Service (DDoS) detection system	▪ Improvement of the network security reporting, monitoring, and measurement system
▪ Continue to develop network service automation ▪ Continue to develop strategies for leveraging AI to improve the efficiency, reliability, and security of network operations	▪ Deployment of Network Automation Applications and continued work on the Automation development ▪ Develop plans for leveraging AI in network operations
▪ Continue to enhance user access to support tools	▪ Deployment of support tools accessible through the user portal
▪ Engage on international networking activities, including Low Earth Orbit (LEO) satellites, Polar connectivity, Asia Pacific connectivity, Global Network Advancement Group (GNA-G)	▪ Deployment of direct Asia Pacific connectivity to support global research activities

3.1.2 Infrastructure Extension Program (IEP)

In FY27, 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:

FY27 Activities	FY27 Short- and Medium-Term Outcomes
▪ Maintain existing high-speed network connections to government research facilities	▪ Continue to support existing connections to government research facilities that meet the performance needs of the government science community
▪ Planning to transition ownership of existing access connections (IEP connections) to the Government of Canada Science Network (GCSN) to Shared Services Canada (SSC)	▪ Coordinated with SSC for a smooth transition of IEP connections

3.1.3 Identity and Access Management

In FY27, 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:

FY27 Activities	FY27 Short- and Medium-Term Outcomes
▪ Continue to work with Canadian Access Federation (CAF) participants and industry experts to plan service evolution ▪ 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 ▪ Increased community engagement through IAM knowledge sharing

3.1.4 NREN Program

In FY27, 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:

FY27 Activities	FY27 Short- and Medium-Term Outcomes
▪ Connect the unconnected with particular focus on Indigenous institutions ▪ Strengthen NREN collaboration ▪ Extend capacity, redundancy, reliability, and security through provincial and territorial NREN Partners' networks	▪ Launch of NREN Program Call 2 to connect the unconnected with a particular focus on Indigenous institutions ▪ Execution underway for all approved NREN Program Call 1 projects to enable the NREN to create, extend, or improve network and security infrastructure and to develop and retain talent ▪ Planning underway to launch NREN Program Call 3 to enable the NREN to create, extend, or improve network and security infrastructure and to develop and retain talent ▪ Execution underway on projects on routing security, the upgrade and implementation of PerfSONAR networking monitoring tools, and the launch and collection of security metrics across the NREN, supported by CANARIE coordination

3.2 Cybersecurity

In FY27, CANARIE will work to support the improvement of the overall cybersecurity posture of the research and education sector:

FY27 Activities	FY27 Short- and Medium-Term Outcomes
▪ Identify, prioritize, and deliver cybersecurity initiatives driven by data, evidence, and sector-wide risk analysis, including reviewing existing programs and services to ensure value to the community, and a more streamlined delivery model	▪ Cybersecurity initiatives are increasingly shaped by sector-wide data, risk analysis, and evidence, enabling more targeted and impactful investment decisions ▪ Increased participation in cybersecurity services, driven by increased value to participants and reduced barriers to participations
▪ Continue to advance the CanSSOC Threat Feed into a broader national Threat Intelligence service, integrating technical indicators, contextual briefings, emerging-threat insights, and automated detection rules	
▪ Complete the 4th cycle of the National Cybersecurity Assessment (NCA), including both operational and strategic enhancements ▪ Build on the success of the NCA to include a more strategic suite of cyber risk modelling services and relevant templates	▪ Stronger shared insights support improved coordination, collaboration, and collective action on the highest-priority risks across the R&E community
▪ Expand the new sector-wide collaboration portal to deliver accurate, timely, and strategically valuable cybersecurity content tailored to the R&E community, including adding capabilities for community-contributed content and peer commentary	▪ Expansion of the collaboration portal's shared library leads to widespread adoption of standardized templates, frameworks, and operational resources, reducing duplication and improving sector-wide consistency
▪ Revitalize the CANARIE cybersecurity advisory model ensuring direct community strategic and technical insights ▪ Expand delivery of technical intelligence updates and an annual executive-level threat briefing, and launch a cybersecurity focused webinar series, to share information and strengthen decision-making within institutions	▪ Strengthened engagement and alignment with the community leads to more trusted partnerships and better-informed cybersecurity priorities

3.3 Activities in concert with the Digital Research Alliance of Canada

In FY27, CANARIE will work with the Digital Research Alliance of Canada (DRAC) to support the Government of Canada's Digital Research Infrastructure Strategy:

FY27 Activities	FY27 Short- and Medium-Term Outcomes
▪ Work to integrate CANARIE and DRAC tools and services, including in cybersecurity	▪ Continued work to integrate Federated Identity Management into DRAC's services ▪ CANARIE support for DRAC's data centre networking requirements ▪ DRAC and host sites participating in CANARIE's cybersecurity services, including the National Cybersecurity Assessment
▪ 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	▪ Alignment on cybersecurity governance for the two organizations, including a single individual chairing both organizations' cybersecurity committees

3.4 Activities Supporting Equity, Diversity, and Inclusion

In FY27, CANARIE will work to advance Equity, Diversity, and Inclusion (EDI), both internally and in the programs we deliver:

FY27 Activities	FY27 Short- and Medium-Term Outcomes
▪ Work in Canada and internationally to support underserved communities ▪ Ongoing Indigenous community engagement strategy and activities ▪ Continued use of institutional EDI plans as an adjudication criterion for funding selection, where appropriate	▪ Launch of NREN Call 2 to connect unconnected institutions, with a focus on indigenous institutions, to the NREN ▪ Continued engagement with submarine Arctic cable consortia and LEO provides to support Northern Connectivity
▪ Training for CANARIE staff on topics that advance EDI ▪ Continued work to renew CANARIE policies, procedures, and practices	▪ Ongoing support for CANARIE Employee Resource Groups ▪ Deliver additional training for staff as appropriate

4. Program Delivery Timelines

		Fiscal year 2026-27			
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, completes 400Gbps capabilities west and south of Montreal - Milestone 8: Removal, cleanup complete of old equipment. **End of Optical System Refresh Project**		***2020-04-01***	***2025-10-24*** **(2025-08-22)** ***2025-01-16*** **(2025-09-26)** **2026-02-20 (2025-11-28)**	**2026-02-20 (2025-11-28)**
	Increase capacity, redundancy, reliability Request For Product (RFP) launches: - Upgrade selected 100Gbps managed services to 400Gbps - Upgrade 10Gbps Atlantic region managed services to 100Gbps - Upgrade Northwest Territory managed service to 1Gbps		**2026-04-01**	**2026-05-08** **2026-06-19** **2026-05-08**	**2027-03-26** **2026-10-30** **2026-08-21**
	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 - Milestone 4: Platform initiated network configuration for SuperComputing Conference 2026 researcher demo		***2023-04-01***	***2025-03-28*** **(2025-05-30)** **2026-05-29 (2025-09-26)** **2026-09-18 (2026-02-26)** **2026-11-15**	**2030-03-31**
	Engage on international networking activities - Agreement for deployment of direct Canada to Asia Pacific connectivity		**2026-04-01**	**2026-07-01**	**2027-03-12**

Eligible Activities	Initiatives	Ongoing	Projected or *Actual* Launch	Major Milestones (Previous)	Projected Completion (Previous)
Network Program (Continued)	Upgrade of the Distributed Denial of Service (DDoS) detection system of the CANARIE network **Was delayed by 1 year as a budget measure.** - Milestone 1: Selection of vendor for equipment, services - Milestone 2: New DDoS system in operation - Milestone 3: Tuning complete, in production		**2026-04-01 (2025-04-01)**	**2026-08-28 (2025-08-29)** **2026-11-27 (2025-11-28)** **2027-03-19 (2026-02-27)**	**2027-03-19 (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***	**2026-03-27 (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*** ***2025-10-31*** **(2025-08-22)**	**2025-02-27** **(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*** ***2025-12-19*** **(2025-12-12)** **2026-02-27**	**2026-03-27**
	Increase availability of and therefore use and value of eduroam, for example at more airports - Milestone 1: Complete consultation with select airports		**2026-04-01**	**2026-06-26**	**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 - Milestone 2: Launch of call to NREN Partners - Milestone 3: Selection of projects		**2025-07-01**	***2025-12-23*** **(2025-12-12)** **2026-04-02** **2026-11-02**	**2029-01-31**
	NREN Call 3 - Milestone 1: Call charter approved - Milestone 2: Launch of call to NREN Partners - Milestone 3: Selection of projects		**2026-02-02**	**2026-03-27** **2026-06-05** **2026-11-20**	**2029-01-31**

Eligible Activities	Initiatives	Ongoing	Projected or *Actual* Launch	Major Milestones (Previous)	Projected Completion (Previous)
Cybersecurity	Threat Feed, National Cybersecurity Assessment, Benchmarking initiatives continued operations for all interested eligible organizations				
	CanSSOC Federated SOC Pilot - Milestone 3 : Data collection complete - Milestone 4: Proposal delivered to ISED		***2023-09-03***	***2025-06-30*** ***2025-09-12***	**2026-08-28**
	IS Assessment NCA data collection platform improvements - Milestone 1: Select vendor - Milestone 2: Improvements complete for launch of 4th year assessments		***2025-04-01***	***2025-12-19*** **(2025-07-25)** **2026-03-27** **(2025-10-31)**	**2026-03-31**
	Perform IS Assessment NCA data collection 4th year assessments - Milestone 1: Data collection complete Add additional cyber risk modelling service - Milestone 1: Select vendor for 3rd Party Risk Management (TPRM) - Milestone 2: Complete pilot for 3rd Party Risk Management (TPRM)		***2025-12-22***	**2026-06-12** ***2025-10-31*** **2026-08-28**	**2026-07-31** **2027-03-26**
	CanSSOC Federated Security Operations Centre - Milestone 1: Funding announcement received - Milestone 2: 30 additional institutions onboarded - Milestone 3: 24 hour operations planning complete		**2026-04-01**	**2026-06-12** **2027-03-26**	**2027-03-31**
	CanSSOC Threat Feed evolution - Milestone 1 : Duplicate McGill hosted threat feed at CANARIE - Milestone 2: Improvements implemented, daily operations transferred from McGill to CANARIE - Milestone 3: integrate additional technical indicators, contextual briefings, emerging-threat insights		***2025-04-01***	***2025-09-26*** **2026-02-20** **2026-06-26**	**2026-03-31** **2026-11-27**
	Expand cybersecurity content available on collaboration portal - Milestone 1 : minimum set of cybersecurity content and refresh interval achieved - Milestone 2: First iteration of community-contributed content		**2026-04-01**	**2026-08-28** **2027-03-20**	**2027-03-31**
	Expand delivery of technical intelligence cybersecurity updates - Milestone 1 : SecuR&E Horizons webinar series launched		**2026-04-01**	**2026-05-04**	**2027-03-31**

Eligible Activities	Initiatives	Ongoing	Projected or *Actual* Launch	Major Milestones (Previous)	Projected Completion (Previous)
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***	**2026-02-27 (2025-07-31)** **2026-04-24 (2025-09-30)**	**2026-05-29 (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, education, and innovation communities. As per the Contribution Agreement, $31.9M is allocated for FY27 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 FY27:

	(in 000s)
Revenues	
Funding	
Government of Canada	31,900
Total Funding	**31,900**
Program Revenues	
Participation Fees	650
Interest Income	50
Total Program Revenues	**700**
Total Revenues	**32,600**
Expenditures	
Program Expenditures	
Network Operations	
Network Infrastructure & Services	15,645
NREN	1,070
CAF	2,089
Total Network Operations	**18,804**
Cybersecurity	
Cybersecurity Programs and Services	6,126
CanSSOC Federated SOC Pilot	1,877
Total Cybersecurity	**8,003**
Total Program Expenditures	**26,807**
Administration Expenditures	5,793
Total Expenditures	**32,600**
Excess of Revenues over Expenditures	-

5.2 Funding Requirements

As indicated in the Program Revenues and Expenditures shown above, CANARIE's cash requirement from the Government of Canada for FY27 is $31.9M.

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 FY27:

	(in 000s)
Program Revenues - Cash	
IEP User Fees - Federal	100
IEP User Fees - Non-federal	6
Participant Fees	544
Total Program Revenues - Cash	**650**
Matching Funds	
Northern Connectivity	860
Total Matching Funds	**860**
TOTAL COST RECOVERY	**1,510**

Throughout FY27, CANARIE will continue to charge fees to users of some 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.
- As part of the initiative to connect Nunavut to the National Research and Education Network, CANARIE supports the cost of Low Earth Orbit Satellite connectivity to Nunavut Arctic College (NAC) and communities within the territory, which is not possible via CANARIE backbone fibre at this time. As part of CANARIE's agreement with NAC, CANARIE funds are matched at a 3:7 ratio.

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.

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 2025. 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

Risk Name	Description	Prob.	Impact	Risk	Mitigation Strategies and Action Plans
CanSSOC Federated SOC Pilot	Risk that CANARIE does not obtain additional funding to continue to expand and run the CanSSOC Federated SOC	M	M	MM	• Submitted a funding proposal that clearly demonstrates the value and feasibility of the Federated SOC, and its alignment with the objectives of ISED, CANARIE, and the community we serve • Frequent communication with ISED and other departments regarding funding request
Corporate IT Breach	A breach of CANARIE's corporate systems could expose financial, contractual, and personal information, and pose reputational risk to the organization	H	H	HH	• Ongoing IT investments • Patching and upgrade practices • DDoS detection • Security awareness training, security monitoring • Incident response plans • Cybersecurity audit program
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	H	H	HH	• Security investments • DDoS detection • MANRS Network Security Norms implemented • Follow Government of Canada guidance with respect to vendors

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 • Security analysts are in place at NREN Partners and working together nationally • Shared cybersecurity framework • NREN security scorecard implemented
Risks of economic conflict (tariff war) between Canada and USA	Changes to tariffs and counter-veiling tariffs on key network equipment may create difficulties for CANARIE in purchasing or renewing contracts with American suppliers, impacting our operations	H	M	MH	• Investigating strategies to address potential currency fluctuation risks • Staying abreast of current economic and political developments and assessing responses to emerging issues • Reviewing risks of pricing fluctuation in existing contracts and structuring new contracts to address any exposure by negotiating terms such as cost increase caps, price adjustment mechanisms, etc. • Reviewing all expiring contracts and possibly alternatives well in advance of renewal dates • Working collaboratively with vendors