CANARIE Annual Business Plan 2024-25

Table of Contents

1 Executive Summary

CANARIE is pleased to present its Annual Business Plan for fiscal year 2024-25 (FY25), the final year of its 2020-25 mandate (assuming the signing of a Contribution Agreement extension amendment for FY25). The document includes past accomplishments as well as CANARIE's plans to achieve its expected results. Risks and risk mitigation strategies are also presented.

1.1 Role of CANARIE

CANARIE connects Canadians to each other and to the world. Our programs equip Canadian researchers, students, and startups to excel on the global stage.

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

Beyond the network, 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 and boost Canada's startups with cloud resources and expertise in emerging technologies.

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

1.2 Focus of Activities: FY25 (April 1, 2024 to March 31, 2025)

CANARIE's focus during the 2020-2025 mandate is on amplifying the impact of Canada's digital infrastructure, as Canadians engaged in data-intensive, collaborative research, and innovation are increasingly dependent on this critical infrastructure.

In FY25, CANARIE will continue to launch and execute programs that build on strong foundations and evolve to support better alignment and integration of the components of Canada's digital research infrastructure, while working to strengthen cybersecurity within the communities we serve.

In addition to the ongoing management of the CANARIE Network and other programs, key planned activities and outcomes for FY25 include:

- Launching new initiatives and continuing the NREN CanSSOC Pilot, to strengthen the cybersecurity of eligible organizations connected to the NREN;

- Ongoing work to support the deployment of 400Gbps capacity on the CANARIE Network;

- Ongoing execution of projects that create, extend, or maintain network infrastructure on regional and territorial partner networks under NREN Calls 3 and 4;

- Development of additional BoosterPacks for the DAIR Cloud environment to catalyze the use of transformative technologies by Canadian SMEs; and

- Ongoing coordination with the Digital Research Alliance of Canada (the Alliance) in support of the Government of Canada's Digital Research Infrastructure Strategy.

1.3 Focus of Activities: 2020 – 2025 Mandate

CANARIE's programming and activities during the 2020-2025 mandate are defined by the following developments that are shifting the research and innovation landscape:

1) the continued digitization of research,

2) the growing need for cybersecurity,

3) the adoption of cloud technologies in all sectors, and

4) the creation and ongoing evolution of the Digital Research Alliance of Canada (the Alliance) to manage the federal investment in advanced research computing, research data management, and research software.

CANARIE activities in the 2020-2025 mandate are focused on the following three areas which directly align with the Expected Results outlined in CANARIE's Contribution Agreement with the Government of Canada:

Network Operations

To deliver a world-class, high-performance network and network-based services, CANARIE will:

a) Increase network capacity and performance to keep pace with the growth in demand;

b) Expand network reach and redundancy to address the needs of research and education communities from coast to coast to coast;

c) Strengthen the overall security posture of the NREN, and better understand its vulnerabilities;

d) Support the development of security capability at NREN-connected institutions; and

e) Evolve the network services portfolio, including identity management, to enhance research, collaboration, and innovation.

Technology Innovation

To bring new collaboration capabilities not previously offered to Canada's research community by creating and funding new software technologies, CANARIE will:

a) Test network-driven and network-enabled technologies to support the research workflow;

b) Drive the adoption of software tools and services to utilize and exploit data (until the end of FY23);

c) Develop new tools and services to support cybersecurity in the research and education ecosystem;

d) Increase the impact of tools and services to users;

e) Support research data management through the development of tools and applications (until the end of FY22); and

f) Promote the collaborative development of data management tools (until the end of FY22).

Private Sector Innovation

To stimulate commercialization CANARIE will:

a) Leverage the network to support innovation, development, and adoption of transformative Information and Communications Technologies (ICT), including DAIR (the Digital Accelerator for Innovation and Research);

b) Facilitate academic and private sector partnerships to drive collaborative innovation and commercialization; and

c) Facilitate access to the CANARIE network to support the CENGN (Centre of Excellence in Next Generation Networks) testbed capabilities across Canada.

2   2023-24 Accomplishments to Date

2023-24 (FY24) is the fourth year of CANARIE's 2020-2025 mandate. The following sections provide an overview of CANARIE's accomplishments in FY24 to date, under each of the three Eligible Activities outlined in the Contribution Agreement that govern the mandate, along with information on outstanding projects for completion. The balance of FY24 accomplishments will be captured in the Annual Report.

2.1 Network Operations

To evolve and expand the CANARIE Network in a flexible and cost-effective manner over the long-term, CANARIE's vision is to deploy fibre from coast-to-coast across Canada. In high-use, high-growth network corridors, CANARIE purchased fibre. This provides the flexibility to add capacity and deploy transformative technologies quickly and at a considerably lower incremental cost, especially as network traffic is returning to pre-pandemic levels and is expected to continue its exponential growth in the future. This connectivity is protected by leased services, which provide necessary network diversity and additional reach.

Thus far in FY24, CANARIE:

- Worked with Nunavut Arctic College to launch the initial set of locations using Low Earth Orbit satellite (LEO) connectivity in the territory, thereby connecting the last jurisdiction in Canada to the NREN

- Deployed equipment to additional segments of the CANARIE Network in support of upcoming 400Gbps capacities

- Continued to roll out *eduroam* wi-fi access authentication through service providers in public, non-institutional environments such as airports and libraries

- Launched the second round of the National Cybersecurity Assessment (NCA) service

- Launched the NREN CanSSOC Pilot

- Hosted the 2023 NREN Assembly to strengthen collaboration among the Canadian NREN Partners

- Hosted the 2023 CANARIE Summit

- Hosted a pilot Canadian SecuR&E Forum, a community focused cybersecurity event for the community

Key projects to be completed or kicked off before the end of FY24 include:

- Begin deployment work for a refreshed optical system in Central Canada

- Begin work to renew eastern dark fibre

- Begin development of network operation management/automation platforms

- Begin assessment of capacity improvement for Northern connections

- Complete the second cycle of the NCA, including the delivery of reports to participant organizations

2.2 Technology Innovation

Research Software and Research Data Management activities have been transitioned to the Digital Research Alliance of Canada, and there have been no activities or outcomes to report for FY24.

2.3 Private Sector Innovation

Under Private Sector Innovation activities, CANARIE leveraged its infrastructure and relationships to support adoption of digital technologies by Canadian SMEs to advance innovation and commercialization.

Thus far in FY24, CANARIE:

- Launched a new DAIR model to support AI-focused users, and expanded the DAIR services catalogue

- Launched a new BoosterPack, which is a free, curated package of resources on a specific emerging technology, built by an experienced Canadian SME

2.4 Innovation Projects

The digital research infrastructure needs of the research, education, and innovation community can (and do) evolve considerably during the term of CANARIE's mandate. Additionally, Information Technology (IT) capabilities or demands on IT continue to evolve, often significantly. For example, current investments in cybersecurity are being driven by the pervasive use of IT in all facets of society which was unforeseen a number of years ago. The CANARIE governance model enables it to respond to evolving ecosystem priorities and needs in a manner that aligns with CANARIE's Contribution Agreement. The role of Innovation Projects is to ensure CANARIE can respond to these new demands.

The inclusion of Innovation Projects is not new for this mandate. In the prior mandate for example, this approach was used to respond to the needs of the community for national Research Data Management (RDM), and also to maximize participation in Phase 1 of the Joint Security Project pilot.

Thus far in FY24, CANARIE:

- Continued with problem identification related to the private sector National Innovation Platform

3 2024-25 Planned Activities

FY25 will be the fifth and final year of CANARIE's 2020-2025 mandate. To deliver on its expected results for the mandate, CANARIE will undertake the following activities in the 2024-25 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.

1) Network Program – As a result of this program, the CANARIE Network will continue to operate and evolve as essential research infrastructure to support research, education, and innovation. To achieve the results of this program, the following activities will be undertaken in the 2024-25 fiscal year:

   i) Operate the Network

   ii) Increase capacity, redundancy, and reliability

   iii) Continue to improve the Network's security posture

   iv) Improve network monitoring activities through the adoption of new tools

   v) Continue to enhance user access to support tools

   vi) Continue to develop software-driven network services

   vii) Operate the Distributed Denial of Service (DDoS) detection system dedicated to the CANARIE Network

   viii) Safeguarding of the Network and CANARIE programs by implementing measures to prevent, detect, and respond to cyber threats, ensuring the integrity, confidentiality, and availability of data and systems

   The following measurable short- and medium-term outcomes will be achieved in FY25:

   - Deployment of additional network capacity to support traffic growth

   - Improved access to commercial cloud services

   - Continued work on the 400Gbps capacity upgrade

   - Continued work on the refresh of the Central and Eastern fibre systems

   - Deployment of additional network capacity to support Northern connectivity

   - Improvement of the network security reporting, monitoring, and measurement system

   - Ongoing improvements to Global Research and Education Network (GREN) Map

   - Deployment of Software Networking Applications

   - Deployment of support tools accessible through the user portal

2) Infrastructure Extension Program (IEP) – As a result of this program, government research institutes will continue to leverage the research network in support of collaborative research with national and international partners. To achieve the results of this program, the following activities will be undertaken in the 2024-25 fiscal year:

i.   Provide existing high-speed network connections to government research facilities

ii. Ensure connections are adequate to meet user needs

The following measurable short- and medium-term outcome will be achieved in FY25:

- Continue to support existing connections to government research facilities that meet the performance needs of the government science community

3) Canadian Access Federation (CAF) Program – As a result of this program, Canada will continue to benefit from robust identity and access management services that enable secure and efficient remote access to distributed resources and tools, anytime. To achieve the results of this program, the following activities will be undertaken in the 2024-25 fiscal year**:**

i.   Continue to work with CAF participants and industry experts to plan how CAF can evolve.

ii. Expand the number of sites that broadcast eduroam in the community to offer options for distance learning and creative utilization of community spaces.

iii. Expand the portfolio of identity-based services, focusing on offering Federated Identity Management as a managed service deployment.

The following measurable short- and medium-term outcomes will be achieved in FY25:

- Increased adoption of 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

4) Cybersecurity Initiatives Program (CIP) and the federal activities of CanSSOC (jointly referred to as the Joint Security Project in CANARIE's Contribution Agreement) – As a result of this program, the overall cybersecurity posture of the sector will be improved. To achieve the results of this program, the following activities will be undertaken in the 2024-25 fiscal year:

i)   Continue to implement existing initiatives and services at eligible organizations

ii)   Design and deliver initiatives to align the research and education sector to a common approach to cybersecurity, and support organizations in maturing their cybersecurity posture

iii) Enhance the Threat Feed service

iv)   Continue the pilot for the CanSSOC shared security operations centre (formerly the Federated SOC) including people, process, and technology components, to inform its deployment across all eligible organizations during the FY26-30 Mandate

v)   Evolve the Intrusion Detection System, including the Intrusion Detection System monitoring and aggregation platform

vi)   Launch the third cycle of the National Cybersecurity Assessment (NCA) service

vii) Launch the second Cybersecurity Initiatives Program (CIP) survey

viii) Work with the Cybersecurity Advisory Committee (CAC) to develop a strategic framework guiding the ongoing evolution of cybersecurity capabilities across the

sector, and to define and implement the next set of initiatives based on the results of the NCA, Benchmarking initiative, and the CIP survey results

    ix) Build on the success of a pilot community focused cybersecurity event held in FY24 and expand to a stand-alone event held in early FY25

The following measurable short- and medium-term outcomes will be achieved in FY25:

- Deploy new initiatives at eligible organizations

- Host community cybersecurity event

- Deploy Security Orchestration, Automation and Response platform (SOAR) to support the NREN CanSSOC pilot

- Increase National cybersecurity analyst capacity across the NREN to support the CanSSOC pilot

- Develop plan to implement the long-term CanSSOC vision

5) NREN Program – The NREN Program initiatives will continue to evolve the NREN such that it acts in a coordinated manner to advance common objectives, while respecting and leveraging the diversity within the federated model. NREN partner engagement will be increased, and initiatives will be better integrated to support this vision. To achieve this, the following activities will be undertaken in the 2024-25 fiscal year:

    i. Extend capacity, redundancy, reliability, and security through provincial and territorial NREN Partners' networks

    ii. Connect research and education facilities

    iii. Strengthen cybersecurity of the NREN

    iv. Strengthen the NREN in the North

    v. Further enhance the processes and capacity of the NREN

The following measurable short- and medium-term outcomes will be achieved in FY25:

- Execution underway for projects defined in the three year NREN FY25-28 Operational Plan (to be revisited on a yearly basis)

- Completion of all approved projects in NREN Calls 2, 3, and 4

- Execution underway to continue establishing the NREN in Nunavut and connect beyond the initial 5 communities

- Increase NREN security through continuation of the NREN SIEM project and continued development of the federated NREN cybersecurity analyst team

- Development and launch of projects to enhance the security of NREN infrastructures

3.2 Technology Innovation

1) Responsibility for Research Data Management moved to Alliance as of March 31st, 2022, and responsibility for Research Software moved to the Alliance as of March 31st, 2022. As such, no activities are expected to be undertaken in 2024-25.

2) Innovation Projects – To support technology innovations and community needs defined

during the mandate, the following activities will be undertaken in the 2024-25 fiscal year:

    i.   Research and identify future projects to be undertaken

The following measurable short- and medium-term outcomes will be achieved in FY25:

- Continued investigation and validation of identified projects ahead of the FY26-30 Mandate

3.3 Private Sector Innovation

The activities undertaken will include delivery of the following programs, along with key initiatives listed under each program:

1) DAIR Program – As a result of this program, CANARIE will continue to leverage the CANARIE Network to support Canadian firms' ability to develop and test innovative ICT applications. To achieve the results of this program, the following activities will be undertaken in the 2024-25 fiscal year:

    i.   Operate the DAIR Cloud platform (embracing updates to the platform core technologies as necessary)

    ii.   Enhance technical capabilities of the DAIR Cloud infrastructure with features to help users reduce time to market

    iii.   Create and publish educational content related to efficient and secure use of cloud resources and services

    iv.   Evolve the DAIR BoosterPack Catalogue to include additional BoosterPacks (training materials and source code developed by Canadian SMEs focused on emerging technologies)

    v.   Cultivate strategic partnerships to add value for the DAIR user community, contributing toward the evolution of a consolidated cloud service

The following measurable short- and medium-term outcomes will be achieved in FY25:

- Increased usage of the DAIR Cloud
- New features added to the DAIR Cloud platform
- Content released to educate SMEs on cloud computing and emerging technologies
- Monitor ongoing cloud usage patterns of SMEs as they develop and test cloud-based applications and services
- Provide additional BoosterPacks, to reduce the time and cost for SMEs to develop new technology skills

Additionally, CANARIE will continue working with its advisory committee, incubators, accelerators, ISED, and other collaborators towards the development of requirements for a National Innovation Platform, and to determine whether a future funding proposal should be developed and approved.

2) CENGN Network Testbed – As a result of this program, the CANARIE Network will be used to foster innovation and commercialization of new ICT technologies in partnership with CENGN. To achieve the results of this program, the following activities will be undertaken in the 2024-25 fiscal year:

i. Ensure network connectivity and related support for the CENGN test bed initiative

The following measurable short- and medium-term outcome will be achieved in FY25:

- CENGN will be able to leverage the CANARIE Network to support advanced testing and demonstration of new ICT products and services

3.4 Activities Supporting Equity, Diversity, and Inclusion

To advance Equity, Diversity, and Inclusion (EDI), the following activities will be undertaken in the 2024-25 fiscal year:

i. Continued use of institutional EDI plans as an adjudication criterion for funding selection, where appropriate

ii. Work with partners in the DRI ecosystem to coordinate joint policy positions on EDI

iii. Training for CANARIE staff on topics that advance EDI

iv. Continued work to renew CANARIE policies, procedures, and practices

v. Ongoing Indigenous community engagement strategy and activities

vi. Work in Canada and internationally to support underserved communities

The following measurable short- and medium-term outcomes will be achieved in FY25:

- Continued engagement with submarine Arctic cable consortia to support Northern Connectivity

- Ongoing support for CANARIE Employee Resource Groups

- Deliver additional training for staff

4 Program Delivery Timelines

			Fiscal year 2024-25		
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 3: Refresh of portion of Central fibre system, begin refresh of Eastern fibre system, add connectivity to commercial cloud, increase capacity to Yukon and add connectivity or capacity to other Territories based on their ability to support.
	    - equipment configuration changes including to reduce energy use.
	      - equipment delivery started on Central fibre system for completion in FY24.
	
	 - Milestone 4: Eastern fibre options review, 400Gbps capable routers installed on main routes.
	
	 - Milestone 5: 400Gbps capable routers installed on ancillary routes
	
	 - Milestone 6: Eastern fibre procurement, optical equipment install underway
			_2020-04-01_	2024-03-24
				 (2023-06-30)
				 (2023-02-24)
				
				 2023-12-21
				 (2023-09-30)
				
				 2024-05-31
				
				 2025-03-31
					2025-03-31
					 (2024-03-31)

	Continue to enhance network security and measurement monitoring tools				
	Continue to enhance user access to support tools - Milestone 4: Global networking map has a live Canadian NREN map display - Milestone 5: Global networking map has a global home for all countries to display their maps - Milestone 6: International maps including Canada available on a single map display		_2023-04-01_	_2023-06-30_ 2024-09-30 2025-03-31	2025-03-31 _(2023-06-30)_
	Continue to develop software-driven network services - Milestone 0: Adapt an existing software system used by other international NRENs. Training sessions provided by ESNET Feb 2024 - Milestone 1: Software driven network operations tests (was automated lightpath tests) completed between an NREN Partner and CANARIE - Delayed. Procurement was completed on software system following international NREN discussions		_2023-04-01_ (2022-04-01) (2021-04-01)	2024-11-01 2025-03-31 (2023-12-15) (2022-11-25) (2022-03-26)	2025-03-31 (2024-03-31)
	Deployment of suport tools accessible through the user portal - Milestone 1: Upgrade Route Registry to current software technologies - Milestone 2: Upgrade Network Operations Portal to current software technologies - Milestone 3: Pilot access by an NREN Partner to routing analysis platform		_2020-04-01_	2024-01-31 (2023-03-31) 2024-05-31 (2023-06-30) 2025-03-31	2025-03-31 (2024-03-31)
	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				

Eligible Activities	Initiatives	Ongoing	Projected or *Actual* Launch	Major Milestones Previous ( )	Projected Completion Previous ( )
CAF 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 CAF services	▓			
	Expand the number of sites that broadcast eduroam wifi in the community - Milestone 2: Managed service technology chosen		*2020-09-01*	**2024-03-01** (2023-03-31)	**2025-03-31** (2024-03-31)
	- Milestone 3: Managed service technology deployed			2024-11-29	
	Research and development efforts focused on expanding identity services	▓			
Joint Security Program (CIP)	DNS Firewall, Intrusion Detection System, Threat Feed, National Cybersecurity Assessment initiatives deployed for all interested eligible organizations	▓			
	Implement Bechmarking and IS Assessment initiatives at eligible organizations - Milestone 2: Information gathered used to assess next initiative		*2021-10-28*	**2023-07-31** (2023-05-26)	**2025-03-31** (2024-03-31)
	- Milestone 3: 2nd year information analysis, national cybersecurity progress results			2024-07-31	
	- Milestone 4: Improvements complete for launch of 3rd year assessments			2024-10-25	
	Next set of Cybersecurity initiatives defined	▓			
	CanSSOC shared security operations centre	▓			
	Security Orchestration, Automation and Response platform (SOAR) - Milestone 1 : Procurement		*2023-09-03*	2024-04-26	2025-04-31
	- Milestone 2: Initial integration into CanSSOC operations complete			2024-11-29	
NREN Program	Execution of approved projects within NREN Call 2 - Milestone 1: Completion of installations		*2021-10-07*	*2023-12-22*	2024-01-31
	- Milestone 2: Project closures			2024-01-31	
	Execution of approved projects within NREN Call 3 - Milestone 2: Completion of installations		*2021-10-07*	2024-12-20	2025-03-31
	- Milestone 3: Project closures			2025-01-31	
	Execution of approved projects within NREN Call 4 - Milestone 2: Completion of installations		*2021-10-07*	2024-12-20	2025-03-31
	- Milestone 3: Project closures			2025-01-31	
	Increase NREN security through continuation of the NREN SIEM project - Milestone 3: renewal of cybersecurity analyst shared funding agreements		*2020-04-01*	2023-11-09	2025-03-31
	Strengthen cybersecurity of the NREN - Milestone 7: Next project selection		*2019-11-28*	2024-06-28	2025-03-31
	- Milestone 8 : Project launch			2024-10-04	
	Strengthen the NREN in the North - Milestone 2: 1st network connection with Nunavut regional network		*2019-08-28*	*2023-08-18* (2023-06-30) (2022-09-30) (2022-03-26)	2025-03-31
	- Milestone 3: Increase connectivity capacity with Yukon regional network			2024-03-31	
	- Milestone 4: Extend to remaining Nunavut regional network sites			2024-09-27	
	NREN Call 3 - Milestone 1: Selection of eligible projects		*2022-10-28*	**2023-05-05**	2025-03-31
	- Milestone 2: Completion of installations			2024-12-31	
	NREN Call 4 - Milestone 1: Selection of eligible projects		*2023-06-01*	*2023-10-03*	2025-03-31
	- Milestone 2: Completion of installations			2024-12-31	

Eligible Activities	Initiatives	Ongoing	Projected or *Actual* Launch	Major Milestones Previous ( )	Projected Completion Previous ( )
Technology Innovation					
Research Software Program	Support and monitor funded projects in platform Call 3 in their maintenance phase - Milestone 5: Project closures		*2019-09-03*	**2024-01-31**	**2024-01-31** (2023-03-31)
Private Sector Innovation					
DAIR Cloud Program	Operate the cloud platform (embracing updates to the platform core technologies as necessary				
	Enhance technical capabilities of the DAIR cloud infrastructure with features to help users reduce time to market				
	Create and publish educational content related to efficient and secure use of cloud resources and services				
	Community forum for the information exchange between private sector innovators				
	Evolve the DAIR BoosterPack pilot project, which utilized a new hybrid cloud environment leveraging private sector investment in Canadian cloud infrastructure/services, and deliver BoosterPack training materials with source code developed by Canadian SMEs - Milestone 3: Continous call for additional BoosterPacks from SMEs - Milestone 4: Additional BoosterPacks available from SMEs				**2024-03-31**
	Cultivate strategic partnerships to add value for the DAIR user community, contributing toward the evolution of a consolidated cloud service - Milestone 4: SME transition between CENGN and DAIR programs more apparent and seamless		*2019-12-11*	**2023-06-30** (2022-12-06)	**2023-06-30** (2024-03-31)
CENGN Network Testbed	Continue network connectivity and related support for CENGN test bed initiative				
Activities Supporting Equity, Diversity, and Inclusion					
EDI	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 $174M to support CANARIE's activities from FY20-FY25 (assuming the signing of a Contribution Agreement extension amendment for FY25). This funding commitment ensures that CANARIE can continue to deliver strategic investments in infrastructure and services for Canada's research and innovation communities. CANARIE has identified a cash flow requirement of $37M for the FY25 funding year.

CANARIE covenants and agrees to hold, invest, administer, and disburse that amount in accordance with the stipulations of the Contribution Agreement. No interest or investment income is payable by the Minister on the funds to be provided.

5.1 Program Revenues and Expenses

The following table summarizes CANARIE's program revenue and expenses projections for the FY25 fiscal year.

	FY25 (in 000s)	Commitments	Total
REVENUES			
FUNDING			
Government of Canada	37,000		37,000
TOTAL FUNDING	**37,000**		**37,000**
PROGRAM REVENUES			
User Fees	623		623
Interest Income	810		810
TOTAL PROGRAM REVENUES	**1,433**		**1,433**
TOTAL REVENUES	**38,433**		**38,433**
EXPENSES			
PROGRAM EXPENSES			
Network Operations			
Network Infrastructure & Services	14,120	1,800	15,920
Network Security	1,631		1,631
Joint Security Project (Cybersecurity)	9,557	3,000	12,557
NREN	6,598		6,598
Private Sector Innovation			
DAIR	2,092		2,092
TOTAL PROGRAM EXPENSES	**33,998**	**4,800**	**38,798**
Administrative Costs	5,550		5,550
TOTAL EXPENSES	**39,548**	**4,800**	**44,348**
EXCESS OF EXPENSES OVER REVENUES	**(1,115)**	**(4,800)**	**(5,915)**

CANARIE has cumulative Excess of Expenses over Revenues from FY21-24. These funds were carried forward to support program and service continuity commitments made in FY24 that will be paid in FY25. Prior to the end of FY25 (the final year of CANARIE's FY20-FY25 mandate) all funds will be spent or committed, and the cumulative Excess of Expense over Revenues will be zero.

5.2 Funding Requirements

As indicated in the Program Revenues and Expenses shown above, CANARIE's cash requirement for FY25 is $37M.

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 FY25.

	FY25 (in 000s)
CASH	
IEP User Fees - Federal	100
IEP User Fees - Non-federal	6
Participant Fees	517
TOTAL CASH	**623**
MATCHING FUNDS	
NREN	1,896
TOTAL MATCHING FUNDS	**1,896**
TOTAL COST RECOVERY	**2,519**

Throughout FY25, 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.

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 Article IV 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 2023. The Investment Policy is guided by the constraints contained in the Contribution Agreement.

6 Performance Monitoring Strategies, Risk Assessment, and Mitigation Strategies

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.

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
Transition and Sustainability Risks	Ongoing Contribution Agreement requirements that have dependency on the Alliance's ability to support the joint work required	M	H	MH	• Working with ISED, the Alliance, and the community to support the development of a fully functional new organization • Implemented project management oversight of C.A. requirements for annual Joint Ecosystem Plan and Ecosystem Report • Meetings are on-going with the Alliance. Relationships with the President, and other key staff at the Alliance, continue to develop and work is on-going
Amendment to Contribution Agreement	Risk that there is no signed amendment to the existing Contribution Agreement ending in March 2024	M	H	MH	• 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
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

Risk Name	Description	Prob.	Impact	Risk	Mitigation Strategies and Action Plans
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) • MANRS Network Security Norms implemented across the majority of the NREN
CanSSOC – NREN Pilot	Risk that the federated model cannot support SOC activities as originally envisioned	M	H	MH	• HR working group • ISL working group • Management oversight • NREN Partner engagement guiding principles adopted