English (Canada)

Cybersecurity Initiatives Program (CIP) Initiatives Application

Eligible Organizations (EOs) that wish to participate in the Cybersecurity Initiatives Program (CIP) must first execute an **Organization Cybersecurity Collaboration Agreement (OCCA)** with CANARIE.

The information included in this form is required for the OCCA. Please review the highlighted areas of the sample Agreement to facilitate completion of this form.

Once your organization's OCCA has been executed, a representative from your regional **National Research and Education (NREN) Partner** will be in touch with instructions for accessing funded initiatives.

Please note: all contact information will be shared with your organization's local NREN Partner.

Please select your province or territory.

Please Select

Organizational and Contact Information

Legal name of your organization: *

For example: The University of Lansdowne's legal name is The Governors of the University of Lansdowne.

Incorporated under the laws of: *

For example: The University of Lansdowne is "… incorporated under the laws of Canada," or "…an educational institution established by the Royal Charter of 1872, as amended."

Organization Type *

For example: A not-for-profit, a corporation, a not-for-profit research institution.

Contact Information

Please provide relevant organization information and contact details as required below. A copy of relevant executed agreement(s) will be sent to each of the provided contacts.

Please note: All contact information provided in this form will be shared with your province or territory's NREN Partner. Once the relevant agreement(s) have been executed, a representative from your regional NREN Partner will be in touch with instructions for accessing funded initiatives.

Organization Address *

Street Address

Street Address Line 2

City

State / Province

Postal / Zip Code

Applicant Contact Name *

First Name

Last Name

Applicant Title *

Applicant Phone Number *

Area Code

Phone Number. Include extension, if applicable.

Applicant Email Address *

example@example.com

Organizational Contact Person for the OCCA Agreement

Please identify the relevant organizational contact person for your organization. This person should be your organization's CIO, CISO, or equivalent. See page 2, section 1. b. of the OCCA Agreement for reference.

Organizational Contact for OCCA Agreement *

First Name

Last Name

Organizational Contact Title *

Organizational Contact Person Phone Number *

Area Code

Phone Number and Extension

Organizational Contact Person Email Address *

example@example.com

Is the address for this individual the same address as provided for the organization (entered above)? *

- Yes
- No

Authorized Signing Authority for the OCCA Agreement

Please identify the relevant organizational Signing Authority for your organization. This person should be your organization's CIO, VP or equivalent. See page 2, section 1. c. of the OCCA Agreement for reference.

Please note: This person must have the authority to legally bind the organization.

Organizational Signing Authority for the OCCA Agreement *

First Name

Last Name

Organizational Signing Authority Title *

Signing Authority Phone Number *

Area Code

Phone Number and Extension

Signing Authority Email Address *

example@example.com

Is the address for this individual the same address as provided for the organization (entered above)? *

- Yes
- No

Second or Alternate Authorized Signing Authority for the OCCA Agreement

If applicable, please provide information for a second or alternate signing authority for your organization. This person should be your organization's CIO, VP or equivalent. If provided, this individual would be included on page 2, section 1. c. of the OCCA Agreement.

Please note: This person must have the authority to legally bind the organization.

Second or alternate Signing Authority: *

- My organization does not have a second or alternative Signing Authority
- My organization has a second or alternate Signing Authority

Second or Alternate Organizational Signing Authority for the OCCA Agreement *

First Name

Last Name

Second or Alternate Organizational Signing Authority Title *

Second or Alternate Signing Authority Phone Number *

Area Code

Phone Number and Extension

Second or Alternate Signing Authority Email Address *

example@example.com

Is the address for this individual the same address as provided for the organization (entered above)? *

- Yes
- No

Second or Alternate Signing Authority Address *

Street Address

Street Address Line 2

City

State / Province

Postal / Zip Code

Funded Initiative Selection

Please select the funded initiatives that your organization would like to implement.

CIRA DNS Firewall

The CIRA DNS Firewall is a simple-to-implement and powerful tool that protects your network by adding an extra layer of protection to safeguards you already have in place. It does this by:

- Blocking/redirecting users (and bots) from accessing malicious sites that contain viruses and malware or are engaged in phishing
- Blocking malware and phishing
- Aggregating threat data to allow/deny access based on real-time threat intelligence
- Reporting malicious activity
- Mitigating risks by locating and quarantining infected devices

CIRA DNS Firewall

- ◯ My organization requests the CIRA DNS Firewall
- ◯ My organization does not request the CIRA DNS Firewall

CanSSOC Threat Feed

The CanSSOC Threat Feed delivers sector-specific threat intelligence to research and education organizations. It aggregates and curates threat intelligence from public and private cybersecurity organizations and open- source feeds into a single block/allow list that can deploy directly in your existing firewalls.

For research & education organizations, the CanSSOC Threat Feed:

- Strengthens your existing protections by adding actionable threat intelligence, purpose-built for research & education organizations.
- Easily integrates into most next-generation firewalls (Palo Alto, Fortinet FortiGate, and Cisco Firepower) to automatically block malicious IP addresses, URLs, and domains.
- Delivers cost savings by leveraging commercially available threat intelligence and feeds.
- Provides the option to feed threat data back into CanSSOC, strengthening the intelligence provided to the whole sector.

CanSSOC Threat Feed

- ◯ My organization requests the CanSSOC Threat Feed
- ◯ My organization does not request the CanSSOC Threat Feed

CanSSOC Threat Feed - Next Steps

Once your organization's OCAA agreement with CANARIE has been executed, we will send your Signing Authority an additional agreement, the **CanSSOC Confidentiality Agreement**.

To complete the CanSSOC Confidentiality Agreement, we require the following:

1. The contact details for your Primary Cybersecurity Contact who will be contacted for an approximately 2-hour technical onboarding session to implement the CanSSOC Threat Feed. The onboarding session typically occurs within 4-12 weeks of the Agreement's execution.
2. Confirmation or addition of the Signing Authority who will execute the CanSSOC Threat Feed Confidentiality Agreement.

After your Agreement has been executed, your local NREN Partner will contact you to schedule a technical onboarding session to implement the CanSSOC Threat Feed.

Primary Cybersecurity Contact for the CanSSOC Threat Feed *

First Name | Last Name | Title

Primary Cybersecurity Contact Phone Number

Area Code | Phone Number. Include extension, if applicable.

Primary Cybersecurity Contact Email Address

example@example.com

Please select the firewall that the CanSSOC Threat Feed will feed into:

Please Select

Other - please enter the firewall name

CanSSOC Confidentiality Agreement Signing Authority

Please identify the relevant organizational Signing Authority for your organization.

Please note: This person must have the authority to legally bind the organization.

Will the Signing Authority for the CanSSOC Confidentiality Agreement be the same as the Signing Authority for the CANARIE OCCA Agreement as noted above?

- ◯ Yes
- ◯ No

What Happens After You Submit?

Your Signing Authority will be sent the CANARIE Organization OCCA via DocuSign.

If you selected the CIRA DNS Firewall:

- Once the OCCA is executed, your NREN Partner will send you a link to the CIRA portal to start the configuration of the DNS Firewall.

If you selected the CanSSOC Threat Feed:

- Once the OCCA is executed, your signing authority will be sent a copy of the CanSSOC Confidentiality Agreement via DocuSign.
- Once the CanSSOC Confidentiality Agreement is executed, your NREN Partner will contact the Primary Cybersecurity Contact above to schedule the Threat Feed technical onboarding process.

If you selected IDS:

- The CANARIE team will send an IDS Participation Agreement to your Signing Authority via DocuSign.
- Once the Agreement is signed by all parties, we will contact the Cybersecurity/Technical Contact listed above to arrange for onboarding sessions that will introduce you to the initiative and guide you through the equipment order form. This will help you select the IDS server configuration best suited for your existing infrastructure.
- The CANARIE team will send your Cybersecurity/Technical Contact the IDS equipment order form. Submitting the form will automatically send your order to Bell, the vendor that has been selected to supply your IDS hardware.
- The CANARIE team will follow up with you to schedule training for installing, configuring, and operating your IDS.

You can contact cip@canarie.ca to learn about the status of the CIP Initiatives process.