Cybersecurity Initiatives Program:
Joining Forces to Secure Canada's Research and Education Sector

Kevin Parent | CICan Webinar | March 31, 2021

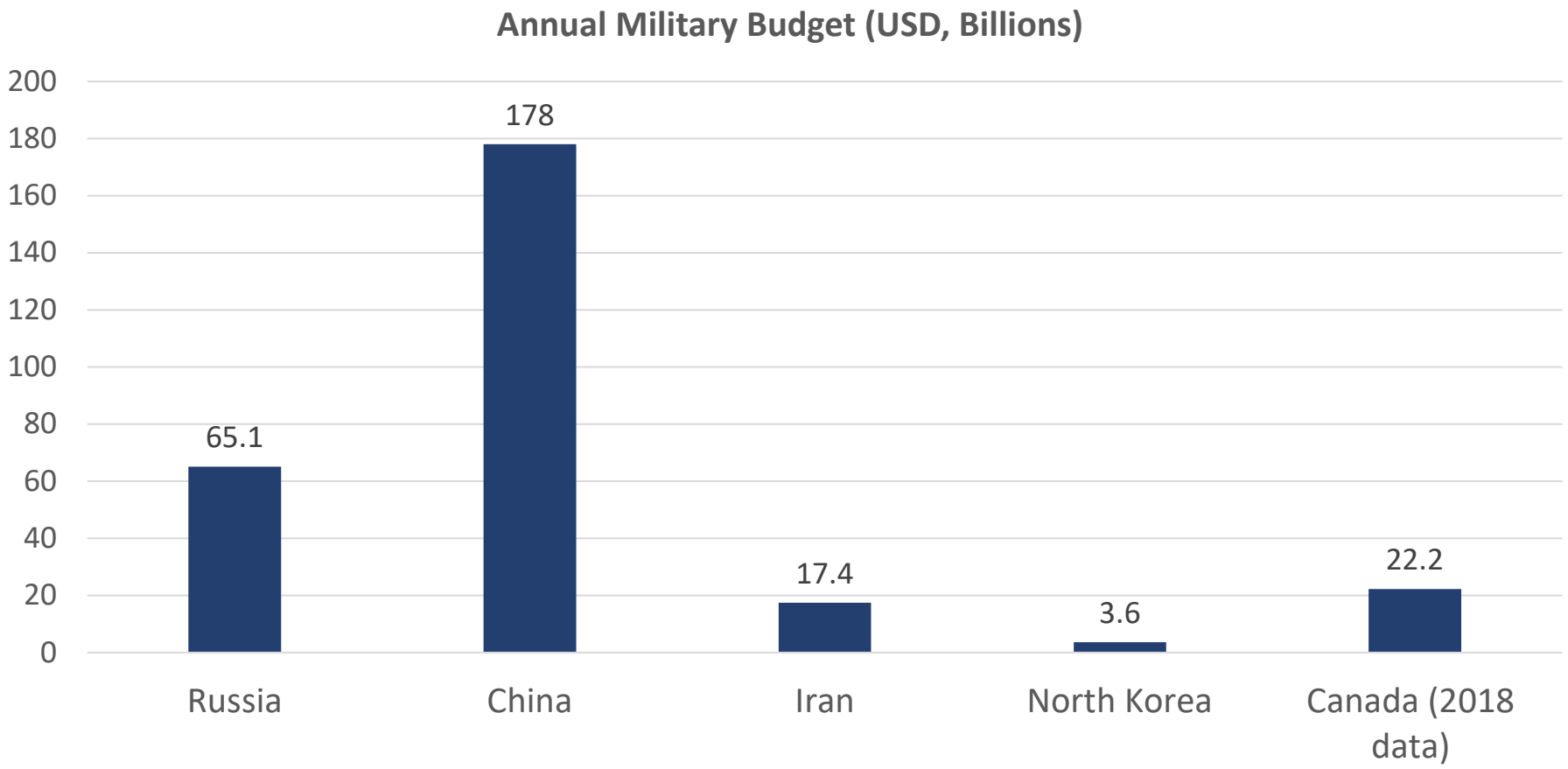
The Problem Statement

"The threat from hostile activity by state actors in all its forms represents a **significant danger to Canada's prosperity and sovereignty.**

CSIS has observed persistent and **sophisticated state-sponsored threat activity** for many years now and we continue to see a rise in the frequency and sophistication of this threat activity…Canada's biopharmaceutical, health, artificial intelligence, quantum computing, ocean technology and aerospace sectors face particularly severe threat activity **because they work largely within academia** and small start-ups."

David Vigneault
Director, CSIS
February 9, 2021

To put the threat in perspective:



*2019/20 annual operating budget for Canada's largest university

Our shared reality

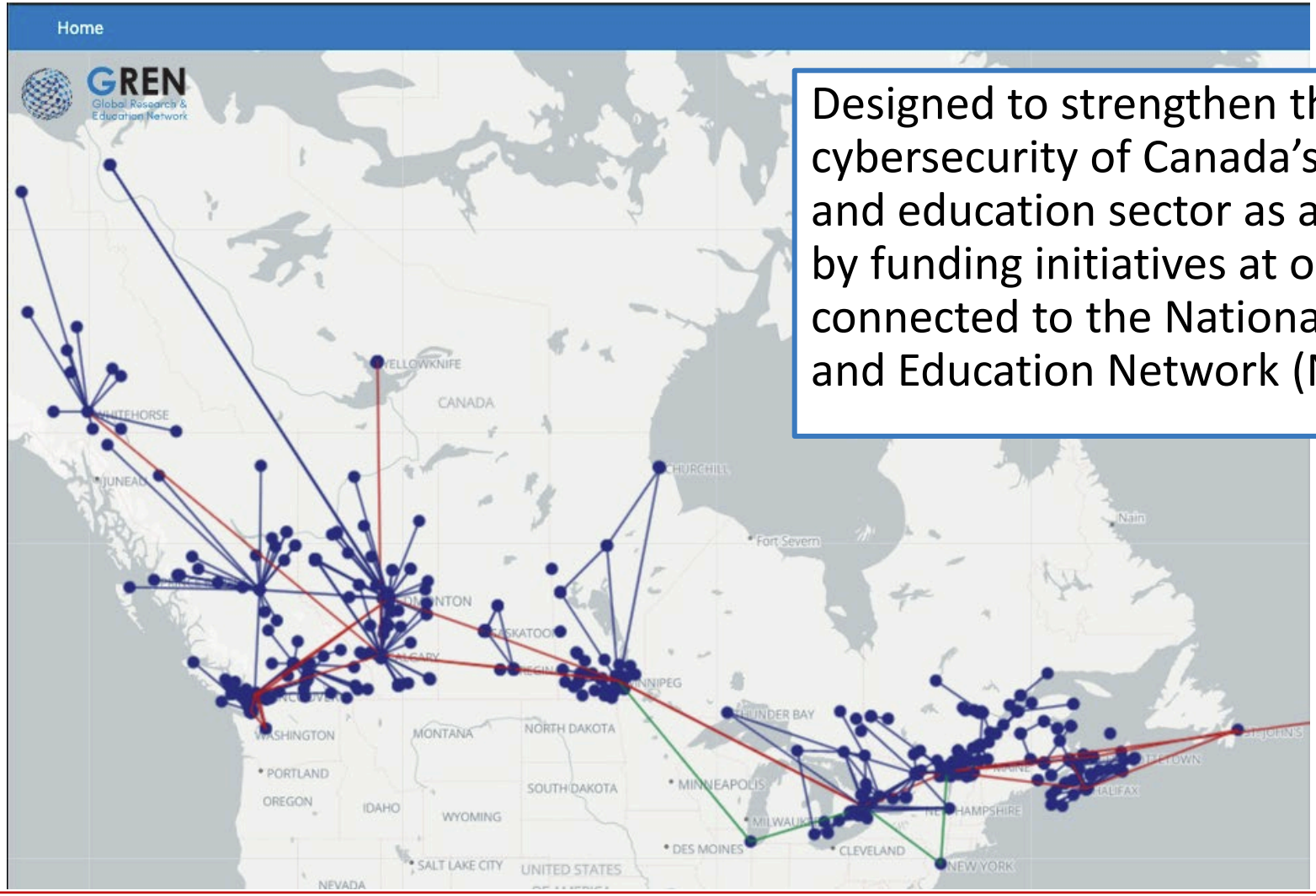
- We are all connected – both physically and by our collaborations.
- Every connected device and organization is susceptible to cyber threats.
- Given our interconnectedness, we're only as strong as our weakest link.
- Cybersecurity is not simply an IT problem – it's an organizational priority.
- A national approach to cybersecurity is only possible when the whole sector aligns and coordinates their efforts.

When it comes to securing the whole sector, we are stronger than the sum of our parts.

Cybersecurity breaches

- There is no shame in being breached!
- Cybersecurity attacks are criminal activities perpetrated by criminals.
- If you are breached, report it and DO NOT pay ransoms!
- Paying the ransom only encourages future attacks. The attackers already have access and there is no guarantee paying the ransom will work.
- Reach out to law enforcement, your NREN Partner, CCCS, CanSSOC. There are many resources to assist. You are not alone.

The Cybersecurity Initiatives Program (CIP)



Designed to strengthen the cybersecurity of Canada's research and education sector as a whole, by funding initiatives at organizations connected to the National Research and Education Network (NREN).

The Vision: A More Secure Canada

The collaboration of our partners has been integral to realizing the vision of the program.

Benefits for eligible organizations:

- Augment your cybersecurity infrastructure
- Measure the impact of cybersecurity initiatives at your organization
- Collaborate with a national community of security experts in R&E
- Increase your team's security capacity and expertise; training & support is integrated into the program

Strengthen the overall security posture of your organization.

At no direct cost.

First 3 Funded Initiatives

cira

D-ZONE DNS FIREWALL

Funding implementation, support, and training across 200+ Eligible Organizations

CANSSOC Threat Feed

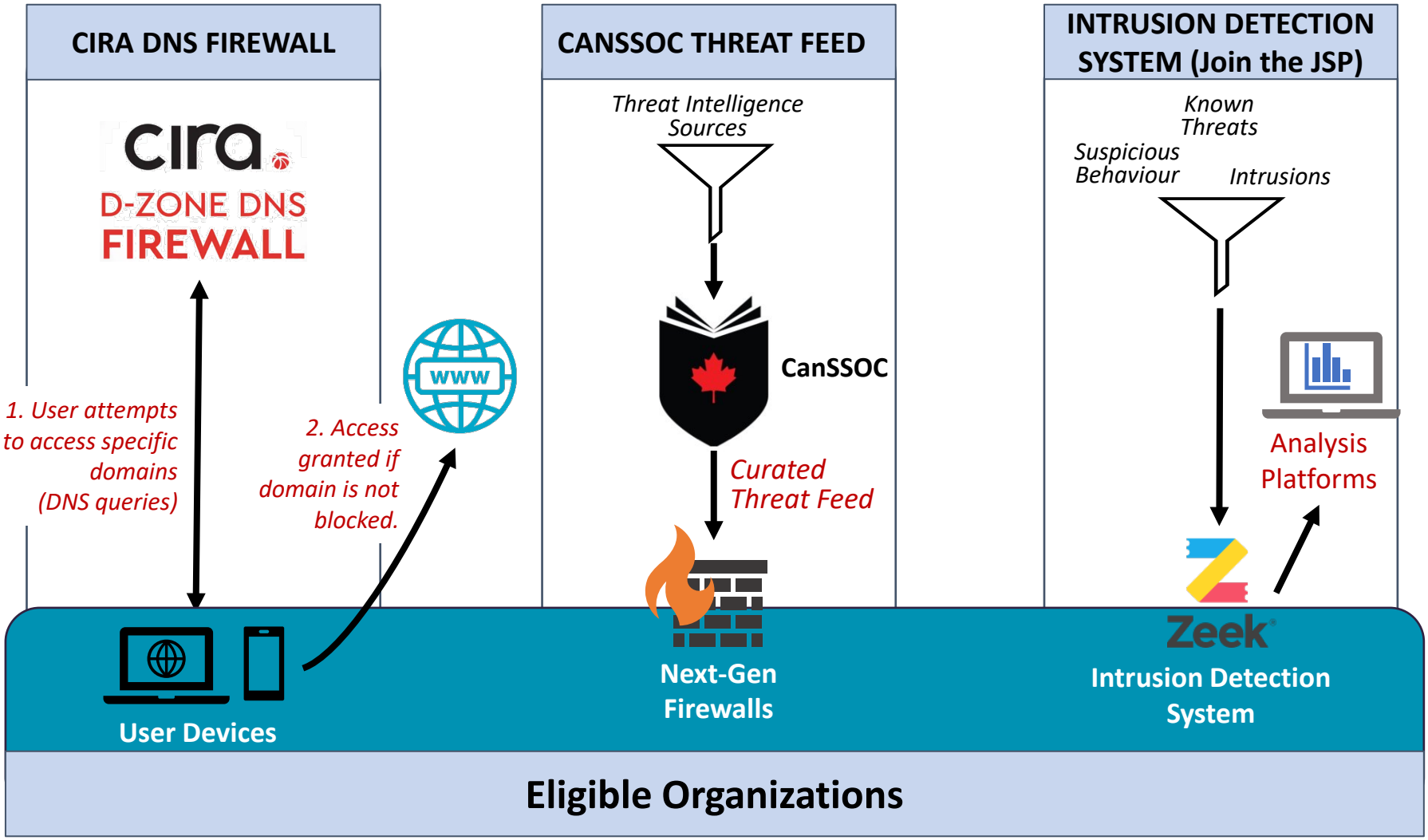
Funding implementation, support, and training across 200+ Eligible Organizations

Intrusion Detection System *(Join the JSP)*

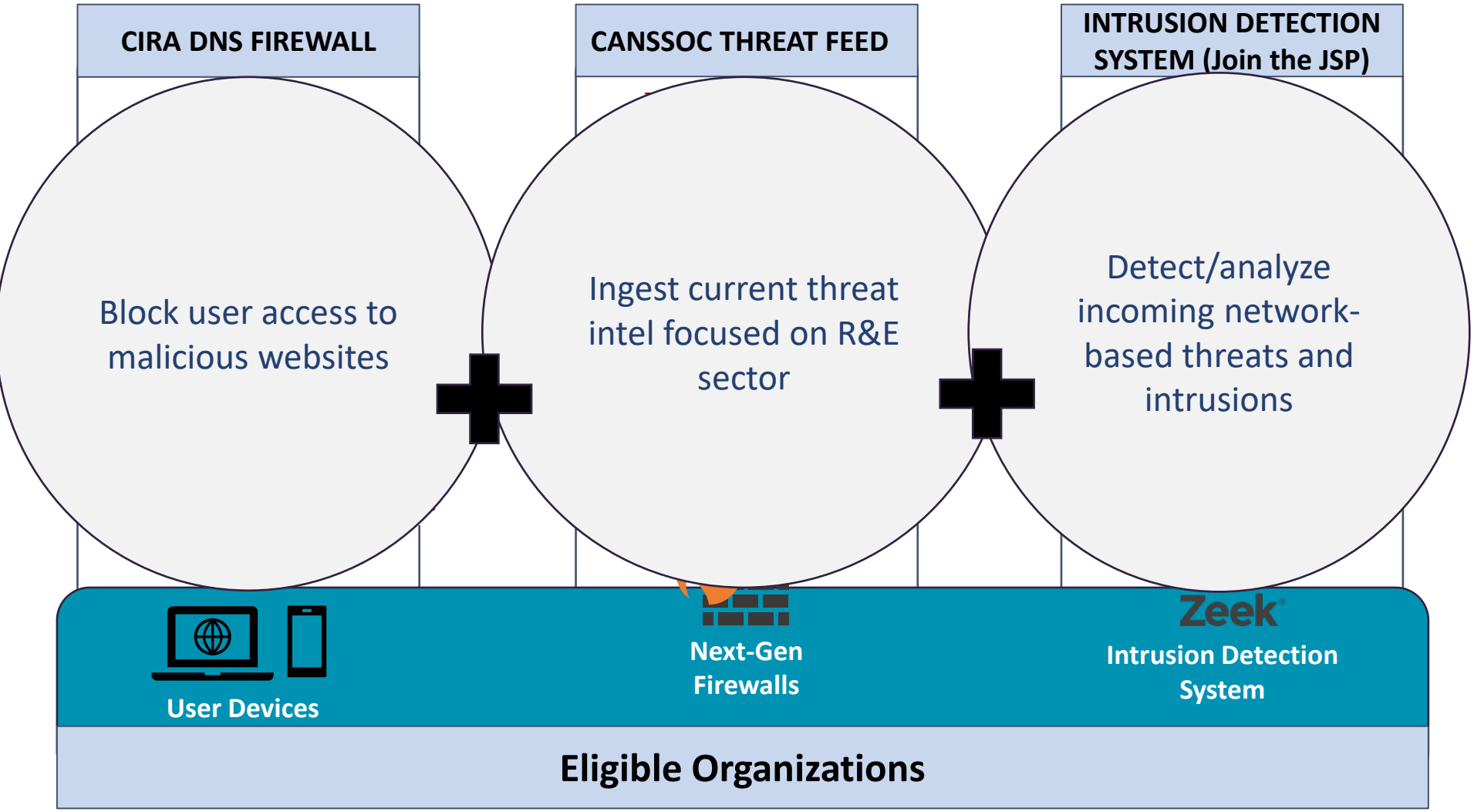
Funding implementation, support, & training for all Eligible Organizations not yet enrolled in the Joint Security Project (JSP)

Intended to integrate with each other to strengthen local cybersecurity and in turn the overall security of the whole sector.

How These Initiatives Fit Together



How These Initiatives Fit Together



Who determines the funded initiatives?

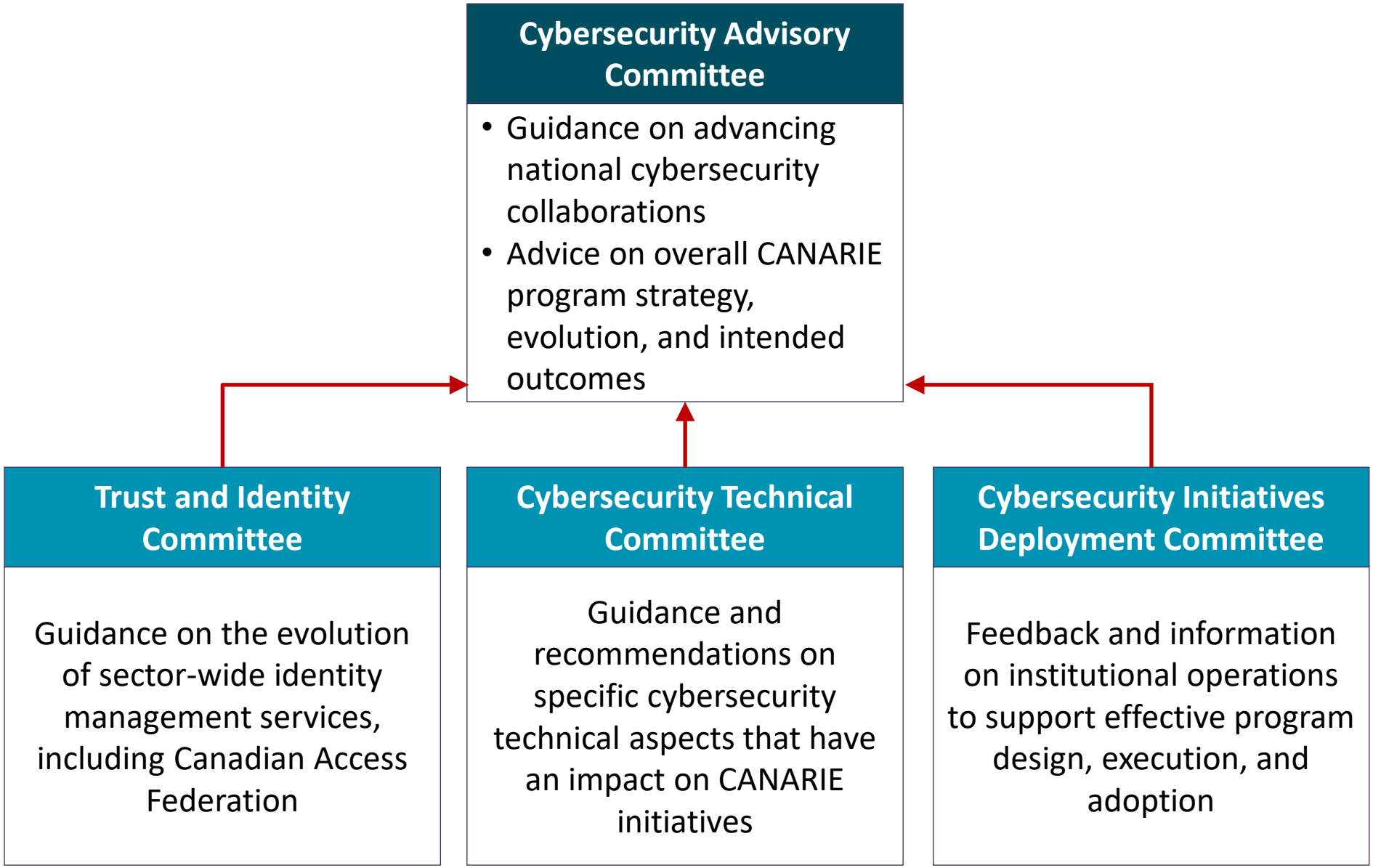
Cybersecurity Advisory Committee

Leaders from Canada's universities, colleges, polytechnics, cégeps, not-for-profit and private sector organizations

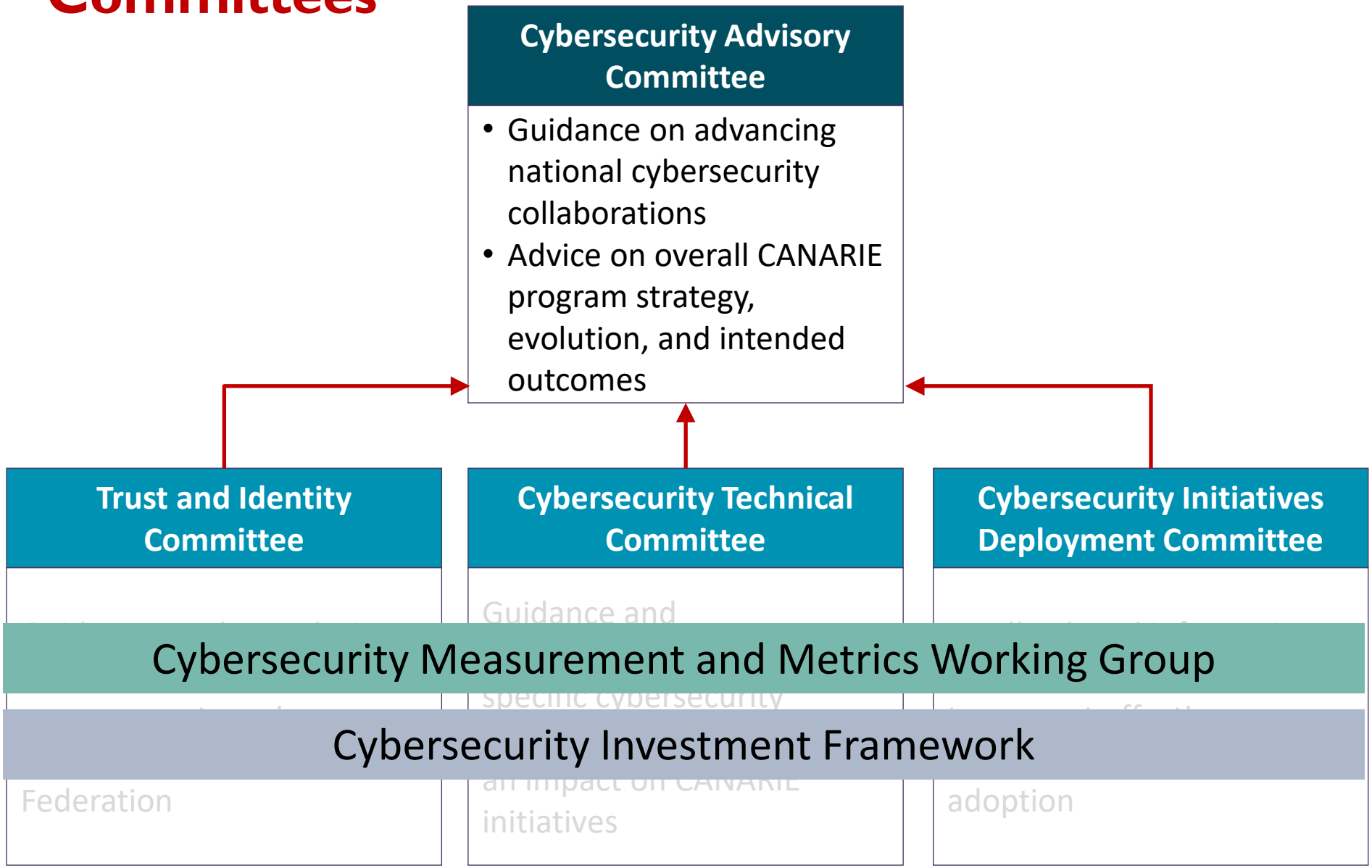
Role:

- advocates for a coordinated national approach to R&E cybersecurity
- provides guidance on funding initiatives under this program

Cybersecurity Initiatives Program Governance



Cybersecurity Advisory Committee & Standing Committees



CICan Member Participation Snapshot

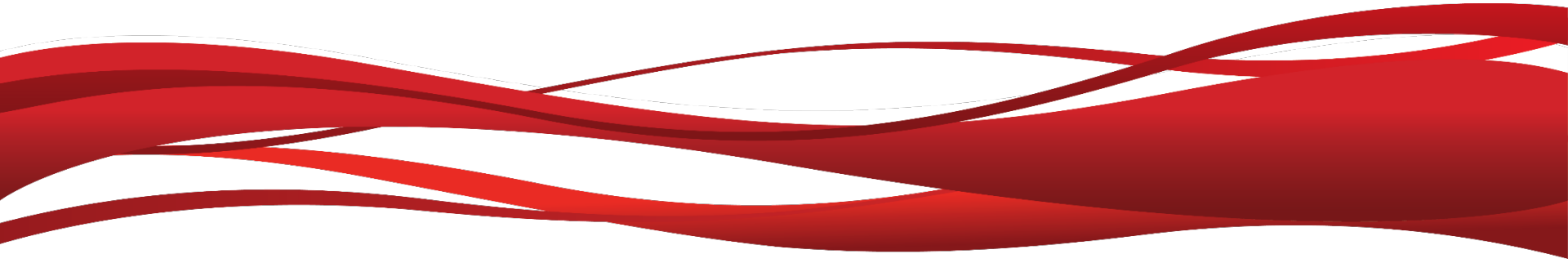
> 102 organizations eligible to participate

- Connected to Canada's National Research and Education Network (NREN); and
- A member organization of an NREN Partner AND connected to that NREN Partner through an autonomous network; and
- A post secondary institution, a non-federal research facility, or a Centre of Excellence.

> 85 currently enrolled in the CIP & ready to benefit from funded initiatives

- 73 organizations using CIRA DNS Firewall

How to Participate



Terminology

NREN

- National Research and Education Network – the country-wide network operated by CANARIE and our provincial and territorial partners

NREN Partner

- One of the 13 provincial and territorial partners in the NREN + CANARIE

Eligible Organization (EO)

- An organization that is eligible to access funded initiatives under the Cybersecurity Initiatives Program

Participant Obligations

- Typically, provide some staff time to participate in initiative deployment and operation
- Contribute metrics through March 2024 for any initiatives deployed by your organization
- Submit a short report after each initiative is deployed

How to Participate

1. Representatives from provincial & territorial NREN Partners will invite eligible organizations to participate in the program
   - Please contact your NREN Partner to confirm your eligibility
   - https://canarie.ca/cybersecurity/cip/support

2. Eligible organizations:
   - Submit a short participation form to CANARIE
   - Execute a standard Organization Cybersecurity Collaboration Agreement (OCCA)

3. Once your OCCA is executed, your NREN Partner will provide instructions for accessing funded initiatives
   - The OCCA only needs to be executed once

Questions you may have…

Do we have to implement all funded initiatives?

> No. You choose the best initiatives for your organization. Please share reasons for opting out of specific initiatives to help planning of future initiatives.

Are these initiatives intended to replace what we already have in place?

> No. The intention is for all eligible organizations connected to the NREN to have a standard baseline of cybersecurity technologies, processes, and skills.

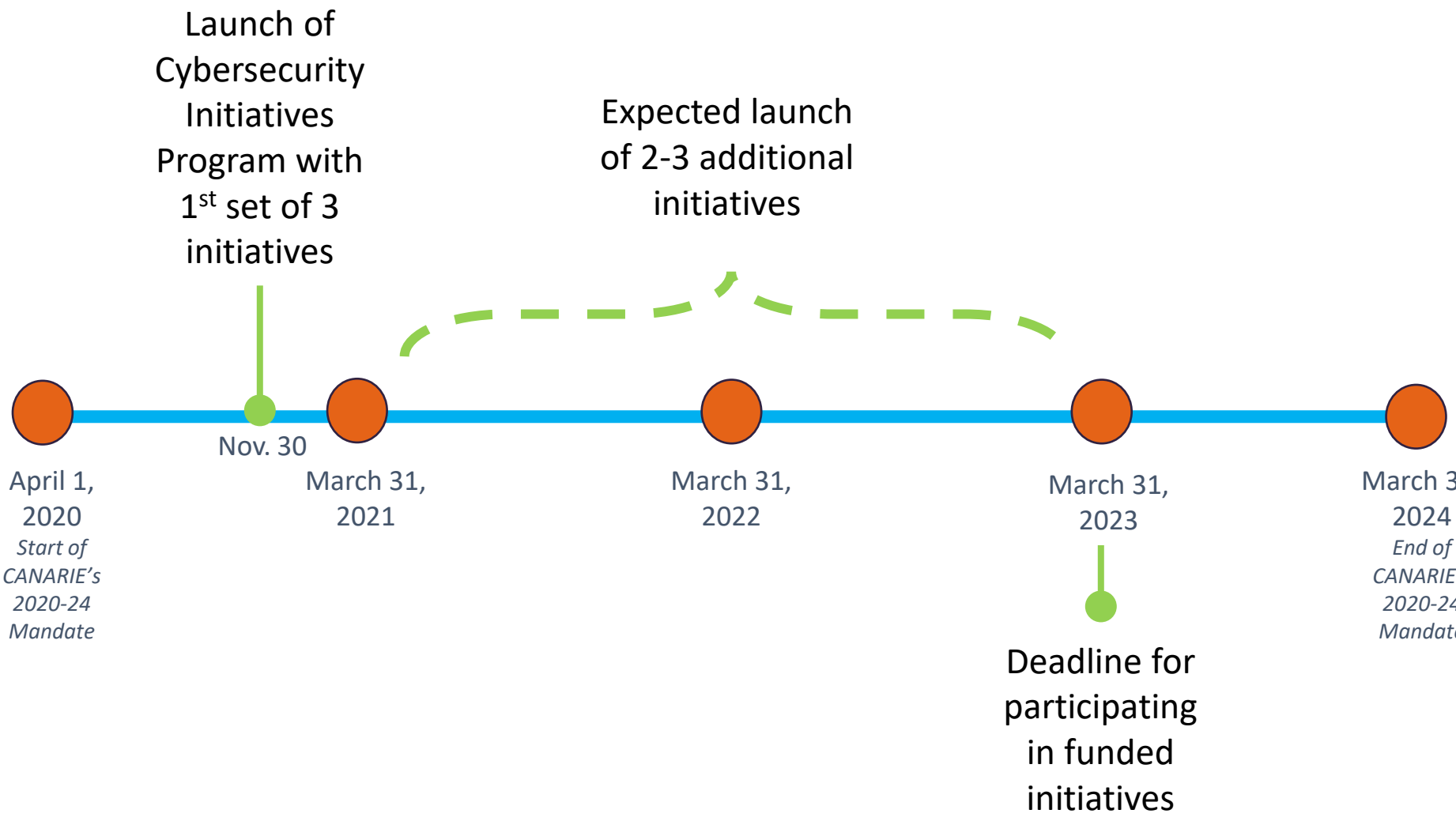
> CIP initiatives are intended to fill gaps that may exist and supplement tools and processes already in place.

Questions you may have…

Is there a deadline to participate in the CIP?

- Participate at any time, but funded initiatives can only be accessed once an OCCA is executed.
- The sooner you participate, the longer your organization will be able to benefit from the funded initiatives.
- Deadline for participation in funded initiatives: March 31, 2023
- Funding for the CIP continues to March 31, 2024

Program Timeline



What's Next?

- CanSSOC Threat Feed launch – coming weeks
- Completion of Intrusion Detection System (previously known as Joint Security Project) – summer 2021
- Engagement with CAC and committees on:
  - National cybersecurity framework reference architecture
  - Next set of priority initiatives
  - Ongoing work on cybersecurity measurement frameworks

Your voice is critical to the success of national, coordinated, collaborative cybersecurity for the R&E sector.

What are your cybersecurity issues/priorities?

canarie

canarie.ca | @canarie_inc