CERT-MU

Computer Emergency Response Team of Mauritius

National Cyber Crisis Management Plan

Instructors:

Dr. Kaleem Ahmed Usmani

Mrs. Jennita Appayya

TLP: White

About CERT-MU

- CERT-MU is a national CERT and operates under the aegis of the National Computer Board, a statuary body under the Ministry of Information Technology.

- It is the second oldest CERT in Africa after Tunisia (TunCERT), set up in May 2008.

- CERT-MU is the main engine driving cybersecurity initiatives in the country.

- It assists the Ministry of Information Technology in the development and implementation of cybersecurity strategies and policies.

- CERT-MU is the FIRST member since 2010.

Structure of Today’s Training:

National Cyber Crisis Management Plan

- Part 1:An Introduction to National Cyber Crisis Management Plan
- Part 2: Inside the Plan – Incident Response: The National Approach
- Part 3: Testing, Implementation and Maintaining the Plan

Part 1

An Introduction to National Cyber Crisis Management Plan

CERT-MU

Cyber Incident

- A cyber incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- It is also an event that threatens the confidentiality, integrity, or availability of Information Systems or institutional data.
- Examples include, but not limited to:
  - ➢Attempts (either failed or successful) to gain unauthorized access to a system or its data
  - ➢Unwanted disruption or denial of service
  - ➢Unauthorized use of a system for the processing or storage of data
  - ➢Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

Significant Cyber Incident or Cyber Crisis

- A significant cyber incident or cyber crisis is an incident or a group of related cyber incidents that together are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of a country or to the public confidence, or public health and safety of the citizens of a country.

The Need for Incident Response (1)

- The increasing reliance on technologies offers many advantages which have improved our economy and quality of life.
- However, it also makes us more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and public safety.
- The frequency of cyber incidents is increasing, and this trend is unlikely to be reversed anytime soon.
- The most significant of these incidents, those likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the country or to the public health and safety of the country.

The Need for Incident Response (2)

- The dependence on well-functioning critical infrastructures points at both the opportunities and vulnerabilities related to the growing use of information and communication technologies (ICT).

- Nations are increasingly facing the need to both stimulate ICT-enabled economies as well as ensure the reliability and security of cyber space, especially when it comes to the protection of critical infrastructure.

- Since the availability, integrity, confidentiality and resilience of critical infrastructures and response to cyber threats have emerged as national priorities for all developed nations, deliberate planning, coordination, and exercising of response activities is necessary in order to minimize the threat and consequences to the nation.

National Capabilities for Incident Response

- National capabilities or readiness is important as it establishes how a nation prevents, protects against, mitigates, responds to and recovers from cyber threats.

- National capabilities include:
  - Legal and Regulatory Measures – (national laws affecting cybersecurity, international obligations)
  - Organisational Measures (national cert, incident response plan, etc..)
  - Technical Measures (incident response tools, forensic capabilities, labs, etc..)
  - Critical Information Infrastructure Protection
  - Financial Considerations (adequate budget, grants, incentives)
  - Implementation Measures (responsibilities and coordination, human resources, finance)
  - Awareness Raising Measures and Education

National Capabilities for Incident Response

To be prepared for a cyber security incident of national significance, it is important to understand the level of threat to the nation and this can be done by:

Assessing the National Cyber Security Landscape

- For the NCMP to be effective, there is a need to assess the cyber threat landscape of the country. To this end, an analysis of the country's cybersecurity strengths and weaknesses should be conducted.
- The following may be considered:
  - ➢Technical infrastructure that supports your critical assets
  - ➢Different types of cybersecurity threats that the country is concerned
  - ➢Sources of these threats such as organised crimes syndicates, state sponsored organisations, extremist groups, etc..
  - ➢Hacktivists, insider threats – or a combination of the possible attack threat vectors
  - ➢Vulnerabilities that may attack critical infrastructure

What is a National Cyber Crisis Management Plan?

- It is an organisational measure and can be defined as follows:

➢ A strategic framework which articulates the roles and responsibilities, capabilities and coordinating structures that support how a Nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure.

➢ A strategic plan which recommends and elaborates on the actions and responsibilities for a coordinated and multidisciplinary approach to respond and recover from cyber security incidents of national significance impacting critical systems and the economy.

Rationale for developing a National Cyber Crisis Management Plan

The rationale for the development of a National Cyber Crisis Management Plan is to:

- Establish roles and responsibilities of the stakeholders during a crisis situation
- Devise ways for incident resolution
- Ensure proper information sharing between stakeholders
- Serve as a basis for improving the management and coordination of cyber incidents at the institutional level
- Set the effective communication channel for message passing related to the incident

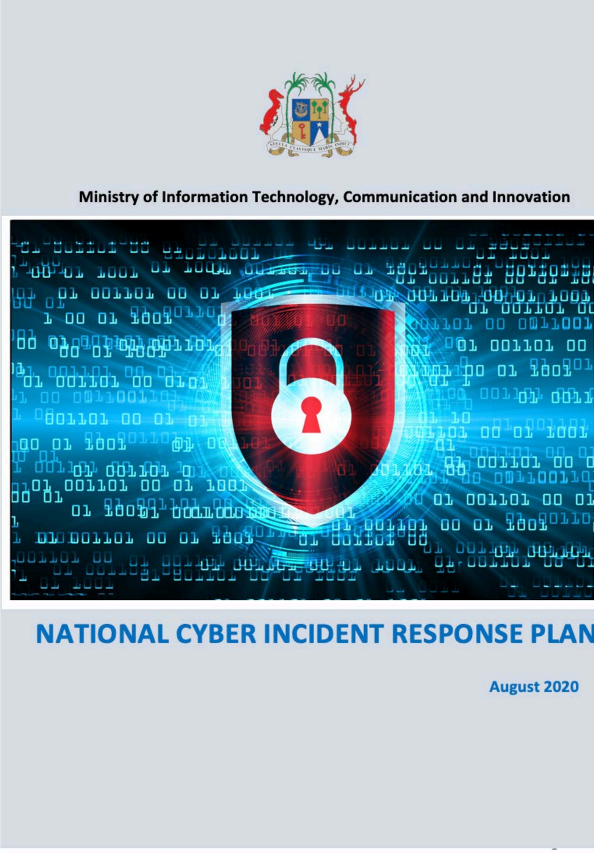
National Cyber Cyber Crisis Management Plan – Country Examples

- Mauritius
- United States of America
- Australia
- United Kingdom
- Canada

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

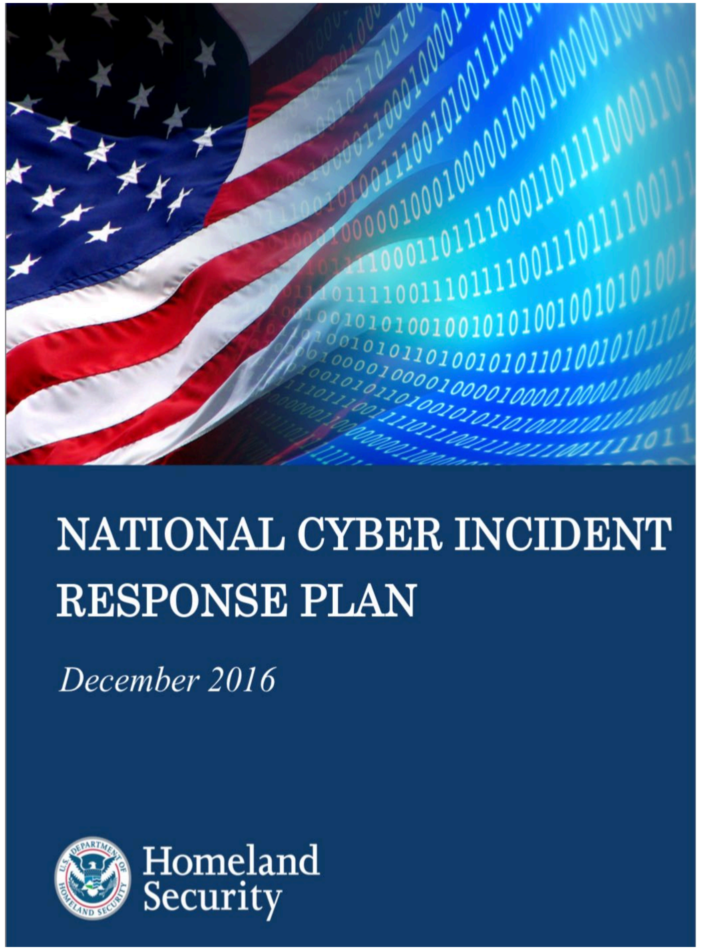
Cyber Incident **Management Arrangements** for Australian Governments



Ministry of Information Technology, Communication and Innovation

NATIONAL CYBER INCIDENT RESPONSE PLAN

August 2020



NATIONAL CYBER INCIDENT RESPONSE PLAN

December 2016

Homeland Security

Objectives of a National Cyber Cyber Crisis Management Plan:

The objectives of a National Cyber Crisis Management Plan are:

- To recommend and elaborate on the actions and responsibilities for a coordinated and multidisciplinary approach to respond and recover from cyber security incidents of national significance impacting critical systems and the economy.
- To minimize disruption of services or loss/theft of information caused by incidents.
- To use the information gained for better preparation or for future handling incidents.

CERT-MU

Applicability of a National Cyber Crisis Management Plan:

- A National cyber incident response plan may depend on country to country and may take many forms and can go into varying levels of detail, depending on the country’s objectives and levels of preparedness or cyber-readiness.

- It establishes the strategic framework and doctrine for a whole-of-Nation approach to mitigating, responding to, and recovering from a cyber incident.

- This approach includes and strongly relies on public and private partnerships to address major cybersecurity risks to critical infrastructure.

- The plan is mainly applicable to the public and private sectors of a

Elements of a National Cyber Crisis Management Plan:

- A National Cyber Crisis Management Plan should be a formal, focused, and coordinated approach to responding to incidents that provides the roadmap for implementing the incident response capability at national level.
- The main elements of the plan are as follows:

  - ➢Vision and Mission Statement
  - ➢Purpose and objectives of the Plan
  - ➢Scope of the policy (to whom and what it applies and under what circumstances)
  - ➢Definition of cyber incidents and related terms
  - ➢The roles and responsibilities of Stakeholders
  - ➢Prioritization or severity ratings of incidents
  - ➢Information Sharing and Communication Methods
  - ➢Metrics for measuring the incident response capability and its effectiveness

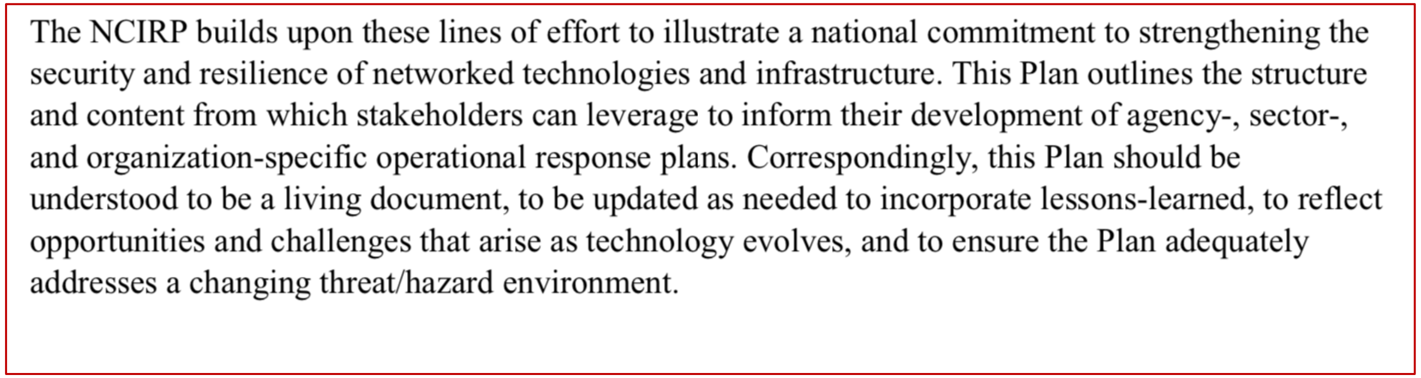
Vision and Mission

- A National Cyber Crisis Management Plan is more likely to be successful when it sets a vision that helps all stakeholders understand what is at stake and why the plan is needed (context), what it is to be accomplished (objectives), as well as what it is about and who it impacts (scope).
- The clearer the vision, the easier it will be for leaders and key stakeholders to ensure a more comprehensive, consistent and coherent approach.
- A clear vision also facilitates coordination, co-operation and implementation of the plan amongst the relevant stakeholders.
- The mission clarifies the purpose and primary, measurable objectives of the plan.

Purpose and Objective

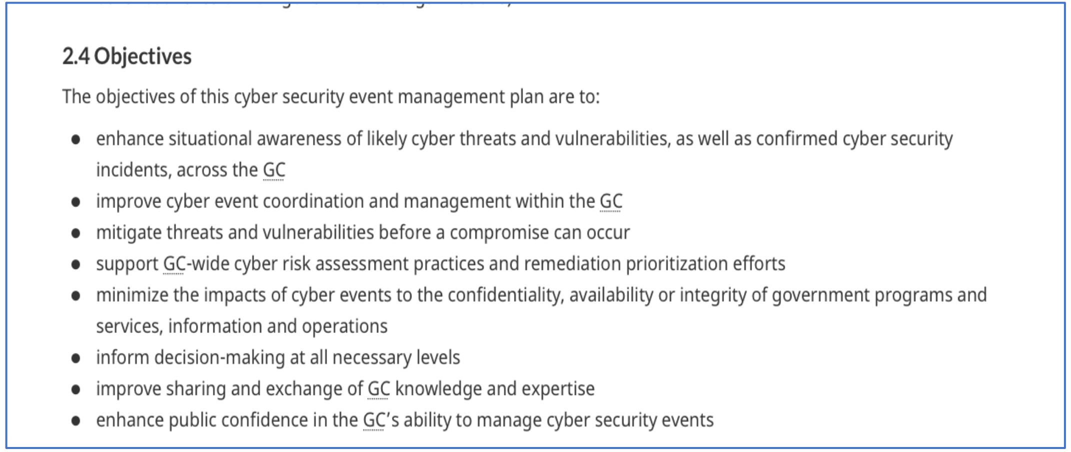
- The purpose and objectives of National Cyber Crisis Management Plan should be clearly stated in the plan
- Examples:

Example 1: National Cyber Incident Response Plan -USA



The NCIRP builds upon these lines of effort to illustrate a national commitment to strengthening the security and resilience of networked technologies and infrastructure. This Plan outlines the structure and content from which stakeholders can leverage to inform their development of agency-, sector-, and organization-specific operational response plans. Correspondingly, this Plan should be understood to be a living document, to be updated as needed to incorporate lessons-learned, to reflect opportunities and challenges that arise as technology evolves, and to ensure the Plan adequately addresses a changing threat/hazard environment.

Example 2: Canada Cyber Security Event Management Plan



2.4 Objectives

The objectives of this cyber security event management plan are to:

- enhance situational awareness of likely cyber threats and vulnerabilities, as well as confirmed cyber security incidents, across the GC
- improve cyber event coordination and management within the GC
- mitigate threats and vulnerabilities before a compromise can occur
- support GC-wide cyber risk assessment practices and remediation prioritization efforts
- minimize the impacts of cyber events to the confidentiality, availability or integrity of government programs and services, information and operations
- inform decision-making at all necessary levels
- improve sharing and exchange of GC knowledge and expertise
- enhance public confidence in the GC's ability to manage cyber security events

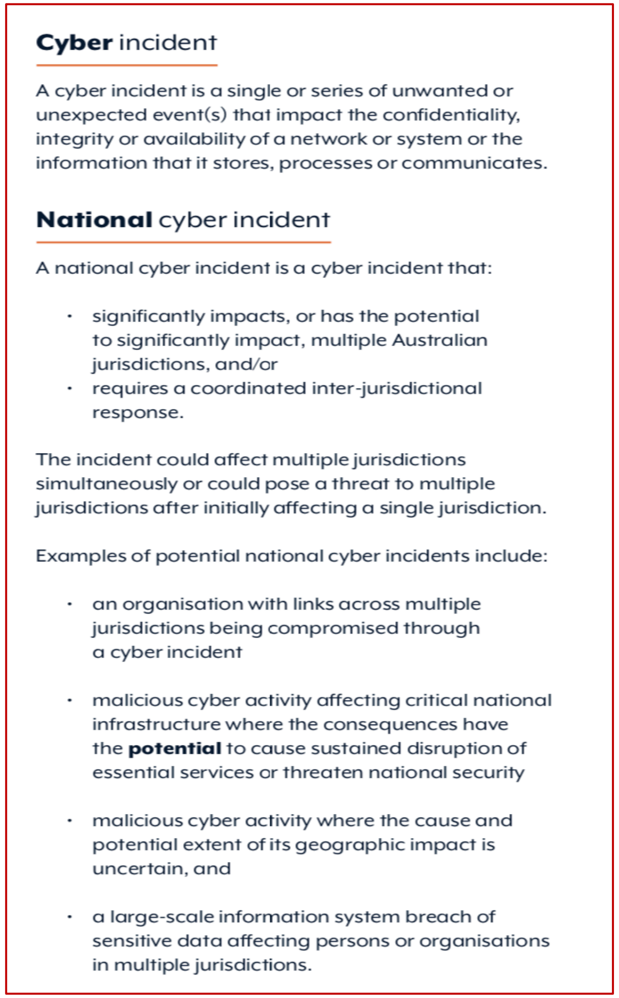
Scope of the National Cyber Crisis Management Plan

- Cyber incident response is an important component of information and communications technology (ICT) and operational technology programs and systems.
- Performing incident response effectively is a complex undertaking and requires substantial planning and resources to establish a successful incident response capability.
- The NCMP provides a consolidated national approach to the management and coordination of potential cyber threats or incidents. It sets out the roles and responsibilities of all stakeholders, critical sectors and other public and private sector in managing incidents of critical in nature.
- It is also a strategic framework for operational coordination among the public and the private sector, and international partners.

CERT-MU

The Need to define a Cyber Incident

- One of the first considerations should be to create NCMP definition of the term “incident” so that the scope of the term is clear.
- This would help in clarifying on the roles of the incident response team, the structures and models
- NCMP development is an important part of establishing a team, so that incident response is performed effectively, efficiently, and consistently, and so that the team is empowered to do what needs to be done.



Cyber incident

A cyber incident is a single or series of unwanted or unexpected event(s) that impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes or communicates.

National cyber incident

A national cyber incident is a cyber incident that:

- significantly impacts, or has the potential to significantly impact, multiple Australian jurisdictions, and/or
- requires a coordinated inter-jurisdictional response.

The incident could affect multiple jurisdictions simultaneously or could pose a threat to multiple jurisdictions after initially affecting a single jurisdiction.

Examples of potential national cyber incidents include:

- an organisation with links across multiple jurisdictions being compromised through a cyber incident
- malicious cyber activity affecting critical national infrastructure where the consequences have the **potential** to cause sustained disruption of essential services or threaten national security
- malicious cyber activity where the cause and potential extent of its geographic impact is uncertain, and
- a large-scale information system breach of sensitive data affecting persons or organisations in multiple jurisdictions.

Australia – Cyber Incident Management Arrangements for Australian Government

Stakeholder Management

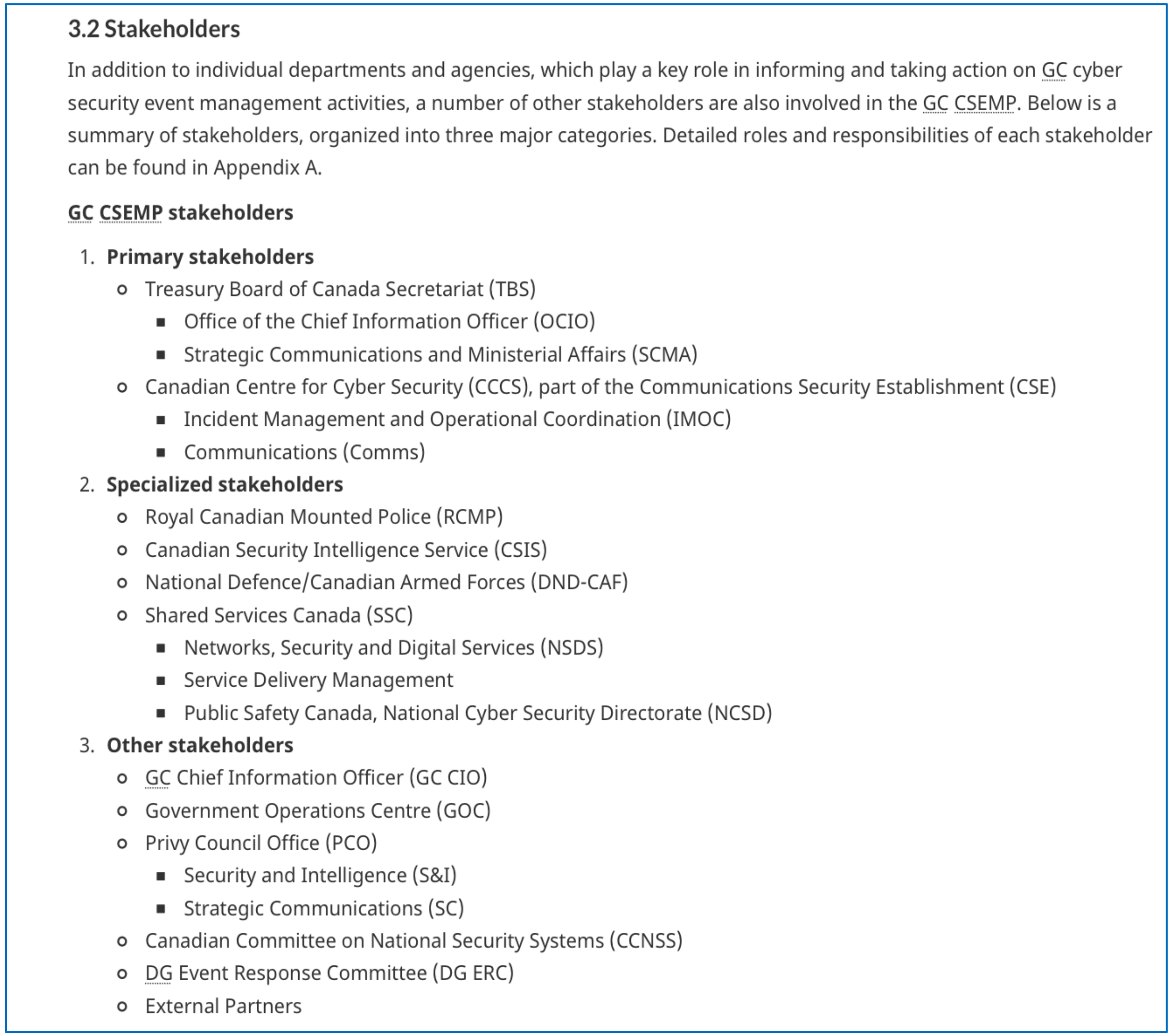
- Cybersecurity is a collective effort and it is important to identify an initial set of stakeholders to be involved in the development of the National Cyber Crisis Management Plan .
- The development, implementation and review of the plan are influenced by a range of elements and played out by various stakeholders
- Examples include government bodies, critical infrastructure operators, private bodies
- Roles should be clarified and outlined how they will collaborate in order to manage expectations throughout the process in order to achieve success.

Roles and Responsibilities of Stakeholders

- Examples of Stakeholders:
  - ➢Law Enforcement
  - ➢Private Sectors – Critical Sectors
  - ➢Internet Service Providers
  - ➢Telco's
  - ➢Vendors

- Outside Stakeholders:
  - ➢Foreign law enforcement agencies
  - ➢CERTs

Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2019



3.2 Stakeholders

In addition to individual departments and agencies, which play a key role in informing and taking action on GC cyber security event management activities, a number of other stakeholders are also involved in the GC CSEMP. Below is a summary of stakeholders, organized into three major categories. Detailed roles and responsibilities of each stakeholder can be found in Appendix A.

GC CSEMP stakeholders

1. **Primary stakeholders**
   - Treasury Board of Canada Secretariat (TBS)
     - Office of the Chief Information Officer (OCIO)
     - Strategic Communications and Ministerial Affairs (SCMA)
   - Canadian Centre for Cyber Security (CCCS), part of the Communications Security Establishment (CSE)
     - Incident Management and Operational Coordination (IMOC)
     - Communications (Comms)
2. **Specialized stakeholders**
   - Royal Canadian Mounted Police (RCMP)
   - Canadian Security Intelligence Service (CSIS)
   - National Defence/Canadian Armed Forces (DND-CAF)
   - Shared Services Canada (SSC)
     - Networks, Security and Digital Services (NSDS)
     - Service Delivery Management
     - Public Safety Canada, National Cyber Security Directorate (NCSD)
3. **Other stakeholders**
   - GC Chief Information Officer (GC CIO)
   - Government Operations Centre (GOC)
   - Privy Council Office (PCO)
     - Security and Intelligence (S&I)
     - Strategic Communications (SC)
   - Canadian Committee on National Security Systems (CCNSS)
   - DG Event Response Committee (DG ERC)
   - External Partners

Governance

- During a cyber security event, the timely engagement of the appropriate level of governance bodies will focus both management and operations to prevent, detect, respond to and recover from cyber security events in a prioritized manner.
- It is therefore important to include in the NCMP, the governance structure that will coordinate and manage incident response and escalation during a cyber crisis.
- Examples of governance bodies are:
  - Cybersecurity Committee
  - Executive Management Team
  - National Cybersecurity Committee
  - Cybersecurity Council
  - Cybersecurity Advisory Council
  - Event Coordination Team

The Incident Response Coordinating Team (IRCT)

- Selection of the Incident Response Coordinating Team
- Structure of the Incident Response Coordinating Team
  - ➢Who forms part of the IRCT?
  - ➢Reporting Structure of the IRCT?

    Example: Mauritius - The Incident Response Coordinating Team reports to the National Disaster Cybersecurity and Cybercrime Committee
  - ➢Functions of the IRCT
- Staff expertise - Incident handling requires specialized knowledge and experience in several technical areas such as knowledge of intrusion detection, forensics, vulnerabilities, exploits, and other aspects of security.

The Incident Response Coordinating Team

- The incident response coordinating team may include several stakeholders such as:
  - Law enforcement
  - CERTs
  - Sectoral Incident Response Teams
  - ISPs
  - Public Safety
  - Technical investigation services
  - Forensics department
- Other stakeholders may also be involved depending on the nature of the incident

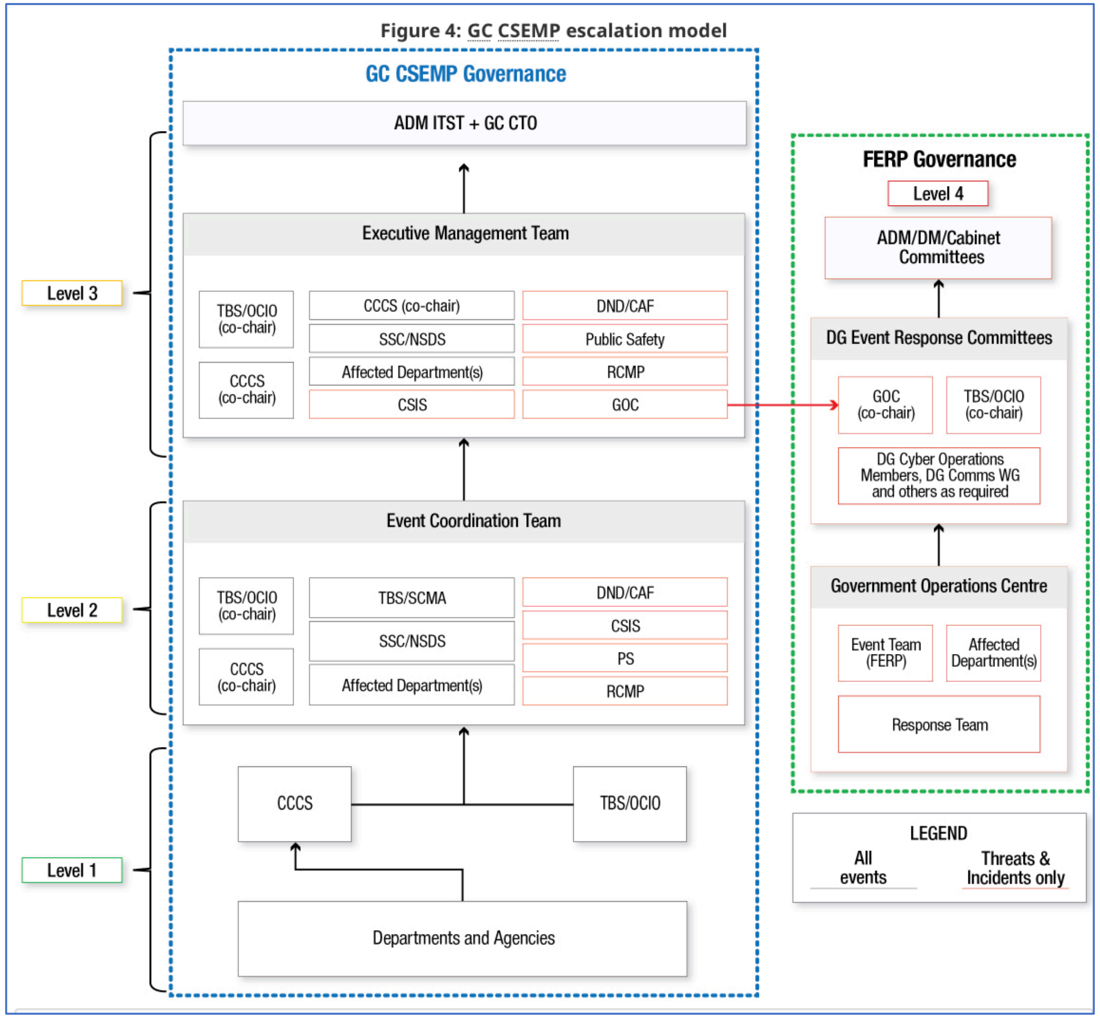


Figure 4: GC CSEMP escalation model

GC CSEMP Governance

ADM ITST + GC CTO

Level 3

Executive Management Team

TBS/OCIO (co-chair)

CCCS (co-chair)

CCCS (co-chair)

DND/CAF

SSC/NSDS

Public Safety

Affected Department(s)

RCMP

CSIS

GOC

Level 2

Event Coordination Team

TBS/OCIO (co-chair)

TBS/SCMA

DND/CAF

CSIS

SSC/NSDS

PS

CCCS (co-chair)

Affected Department(s)

RCMP

Level 1

CCCS

TBS/OCIO

Departments and Agencies

FERP Governance

Level 4

ADM/DM/Cabinet Committees

DG Event Response Committees

GOC (co-chair)

TBS/OCIO (co-chair)

DG Cyber Operations Members, DG Comms WG and others as required

Government Operations Centre

Event Team (FERP)

Affected Department(s)

Response Team

LEGEND

All events

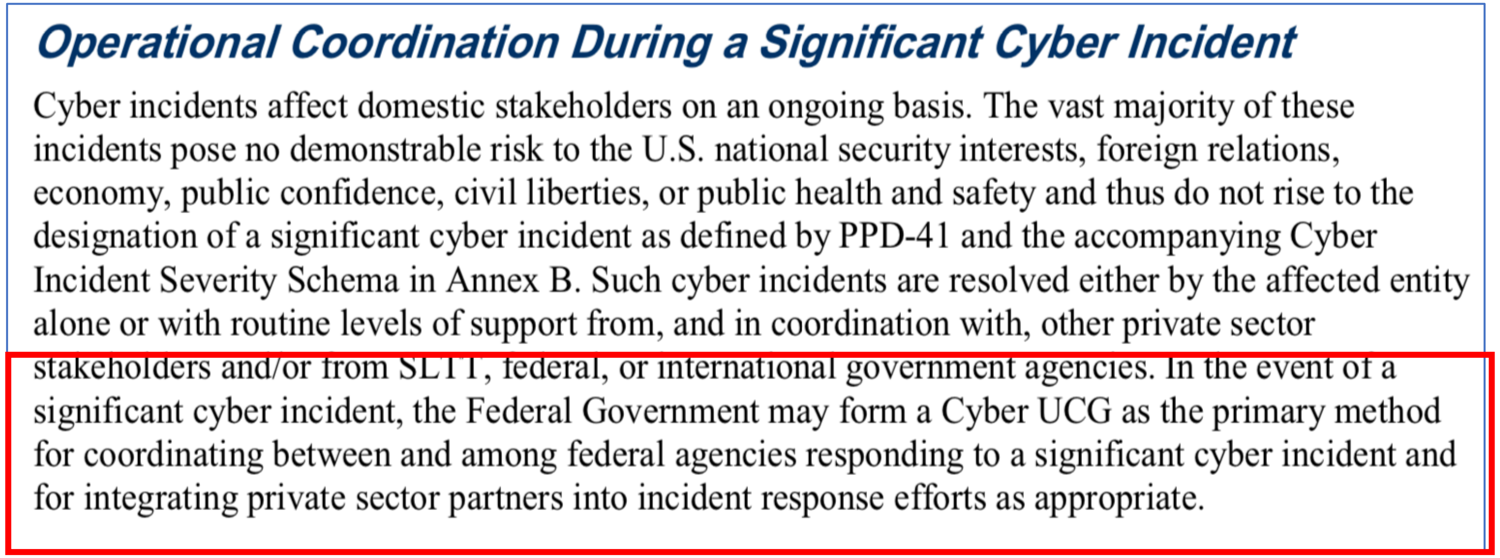
Threats & Incidents only

Eg: Canada Cyber Security Event Management Plan (GC CSEMP) 2019

The Incident Response Coordinating Team

Case Example 2 – USA

- During the event of a significant cyber incident, a Cyber Unified Coordination Group (UCG) is convened
- The Department of Justice, through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), serve as the lead federal agency for threat response activities.



Operational Coordination During a Significant Cyber Incident

Cyber incidents affect domestic stakeholders on an ongoing basis. The vast majority of these incidents pose no demonstrable risk to the U.S. national security interests, foreign relations, economy, public confidence, civil liberties, or public health and safety and thus do not rise to the designation of a significant cyber incident as defined by PPD-41 and the accompanying Cyber Incident Severity Schema in Annex B. Such cyber incidents are resolved either by the affected entity alone or with routine levels of support from, and in coordination with, other private sector stakeholders and/or from SLTT, federal, or international government agencies. In the event of a significant cyber incident, the Federal Government may form a Cyber UCG as the primary method for coordinating between and among federal agencies responding to a significant cyber incident and for integrating private sector partners into incident response efforts as appropriate.

Determining the Incident Severity Level

- One of the most significant element of a NCMP is to determine the incident severity level

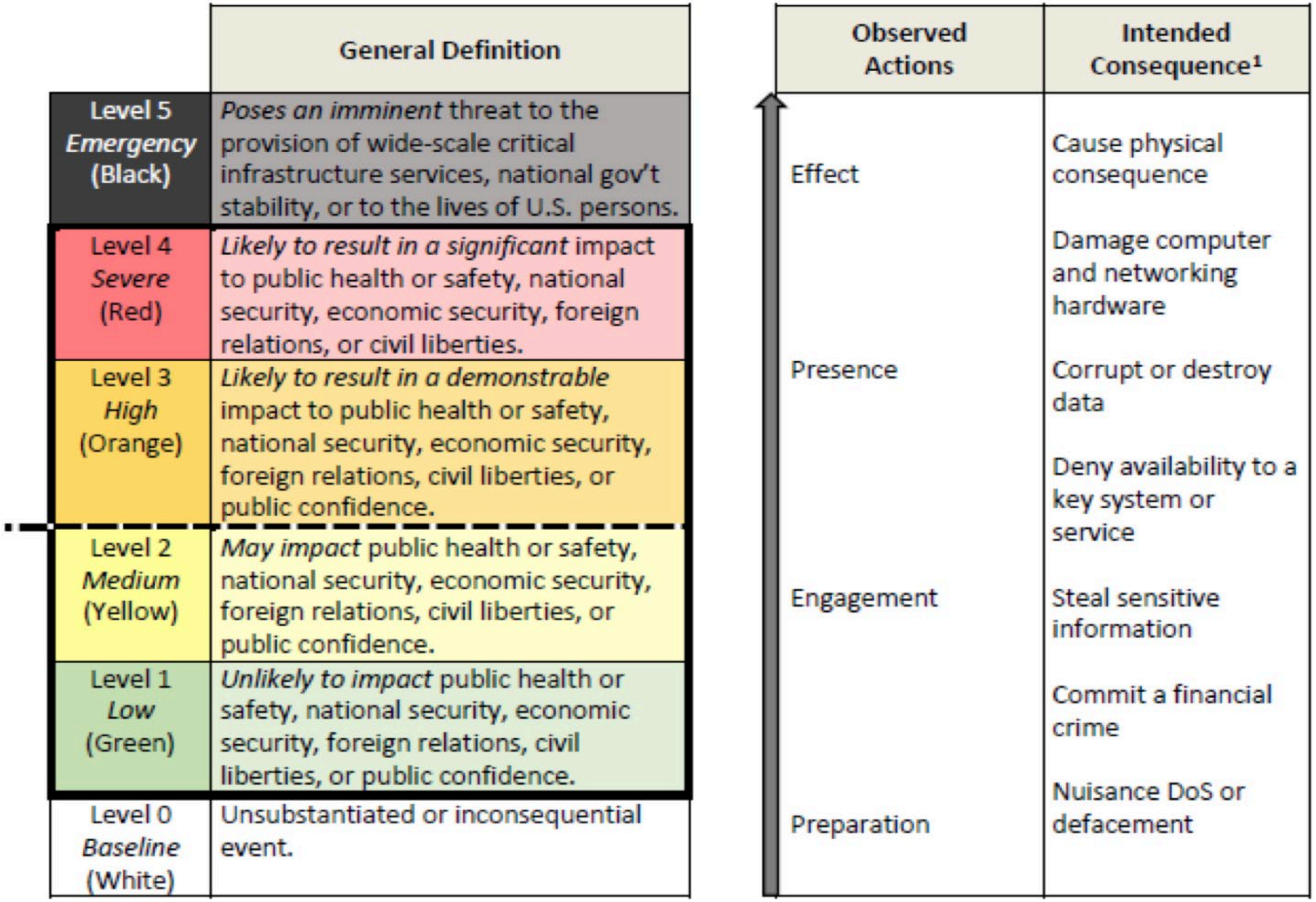
- Development of an incident severity framework

- The framework will help to evaluate and assess cyber incidents to ensure a common view of the:
  - Severity of a given incident
  - Urgency required for responding to a given incident
  - Seniority level necessary for coordinating response efforts
  - Level of investment required for response efforts.

Determining Incident Severity Level

- Example – USA

Cyber Incident Severity Schema



	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

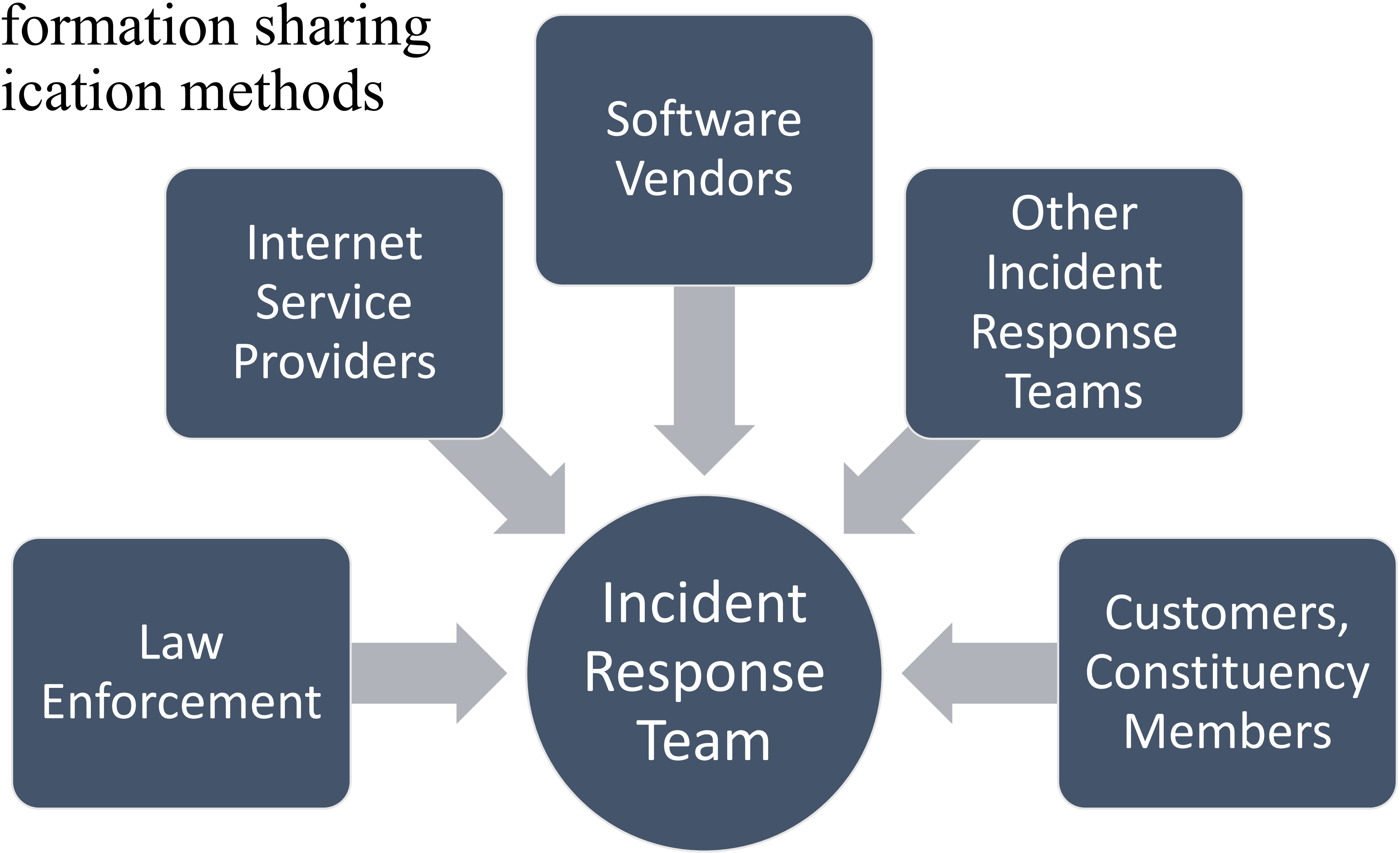
Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

Information Sharing and Communication Methods

- During incident response, there is a need to communicate about the incident to other parties.
- Proper communication methods so that only the appropriate information is shared with the right parties
  - Example: Traffic Light Protocol - created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience.
- Only share relevant incident information with other parties to to improve detection and analysis of incidents.

Information Sharing and Communication Methods

- Parties for information sharing and communication methods


Software Vendors
Internet Service Providers
Other Incident Response Teams
Law Enforcement
Incident Response Team
Customers, Constituency Members

CERT-MU

Thank You

Computer Emergency Response Team of Mauritius (CERT-MU)

CONTACT US

Tel: 210 55 20 | Hotline: 800 2378

General Enquiry: contact@cert.ncb.mu
Subscribe to Mail List: subscribe@cert.ncb.mu

Incident Reporting: incident@cert.ncb.mu
Vulnerability Reporting: vulnerability@cert.ncb.mu

Cybersecurity Portal: http://cybersecurity.ncb.mu
Website: www.cert-mu.org.mu