CERT-MU

Computer Emergency Response Team of Mauritius

National Cyber Crisis Management Plan

Instructors:

Dr. Kaleem Ahmed Usmani

Mrs. Jennita Appayya

TLP: White

Part 2
Inside the Plan – Incident Response: The National Approach

Developing National Cyber Crisis Management Plan

- Today’s training session ultimately aims to provide you with an understanding of the steps to be taken by a nation to respond to an incident of national significance, to prioritize an incident based on its severity level and make use of Traffic Light Protocol for information sharing and communication.

- The Focus will be on Incident Response Lifecycle.

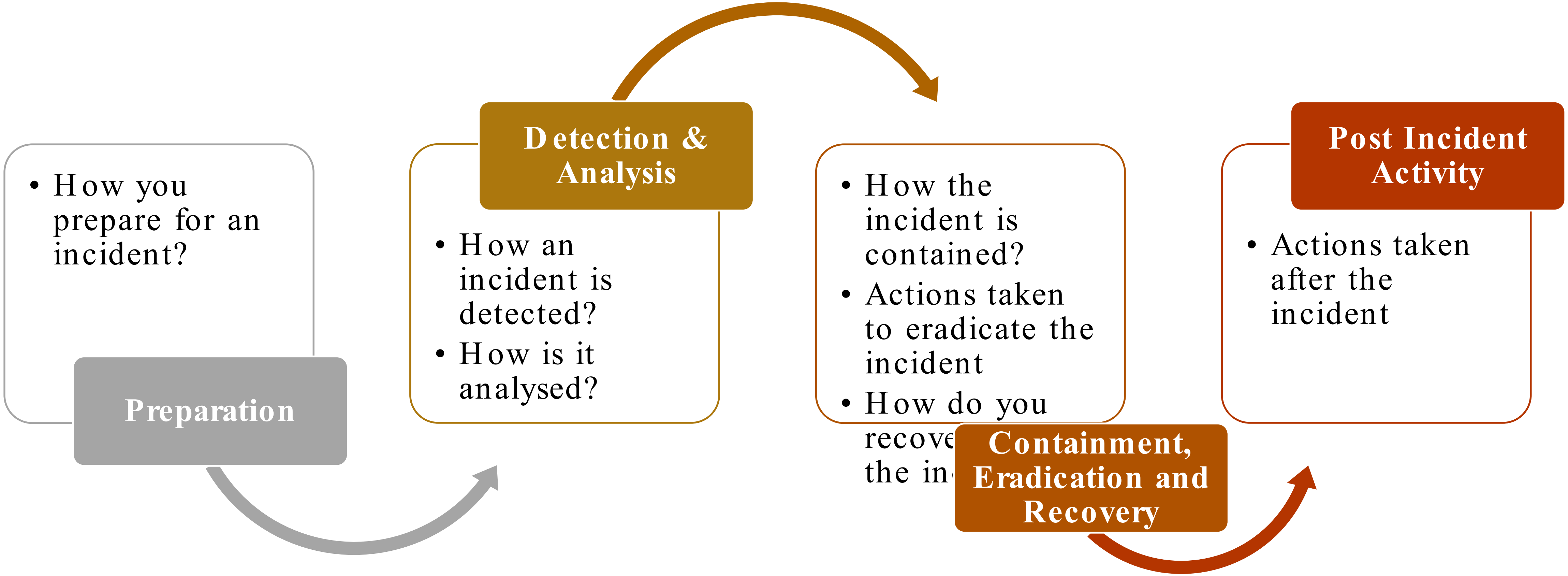
Inside The Plan: Incident Response - The National Approach

Inside The Plan: Incident Response - The National Approach

- The national approach of incident response differs from country to country
- Existing Incident Handling frameworks:
  - NIST
  - SANS
  - ISO/IEC 27005

- Generally, the process of incident handling consists of the following steps:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication and Recovery
  - Post Incident Activity

Inside The Plan: Incident Response - The National Approach



Preparation

- How you prepare for an incident?

Detection & Analysis

- How an incident is detected?
- How is it analysed?

Containment, Eradication and Recovery

- How the incident is contained?
- Actions taken to eradicate the incident
- How do you recove the in

Post Incident Activity

- Actions taken after the incident

CERT-MU

Phase 1: Preparation

- In incident Response, it is very important to be prepared before an incident is detected. It is not only about establishing an incident response capability, but also about preventing incidents or minimizing the impact/damage.
- Preparation includes those activities that enables a Nation to respond to an incident effectively such as policies, tools, procedures, effective governance and communication plans.
- It also implies that necessary controls are in place to recover and continue operations after an incident is discovered.
- The development of a National Cyber Crisis Management Plan is one of the measures of the Preparation phase.
- The country is prepared and have the procedures in place in the event of a cyber incident of national significance.

Phase 1: Preparation

- Some of the measures in the preparation phase include having the capabilities in place to respond effectively to an incident when it occurs.

- This include the following:
  - ➢Legal and Regulatory Measures – (national laws affecting cybersecurity, international obligations)
  - ➢Organisational Measures (setting up national cert, developing incident response plan, etc..)
  - ➢Technical Measures (incident response tools, forensic capabilities, labs, etc..)
  - ➢Awareness Raising Measures and Education (sensitization campaigns, trainings for employees

Phase 2: Detection & Analysis

- This phase deals with the detection or identification of event, which can be made with security tools or notification by an inside or outside party about a suspected incident.
- This is one of the most challenging phase – to detect successfully detect an incident and if so, the type, extent, and magnitude of the problem.
- After an incident is detected, an initial analysis should be performed to determine the incident scope, such as:
  - which networks, systems, or applications are affected
  - who or what originated the incident; and
  - how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited).

Phase 2: Detection & Analysis

- Sources through which an incident may be detected are:
  - IDS, SIEM, anti-virus software, file integrity checking software, logs, third party monitoring services, information on new vulnerabilities and exploits, people from inside and outside, etc..
- Attack vectors may be through: the web, email, removable media, impersonation (man-in-the-middle), improper usage
- This phase also includes the declaration and initial classification of the incident.
- The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident, which also helps in determining whether the incident is of national significance or not

CERT-MU

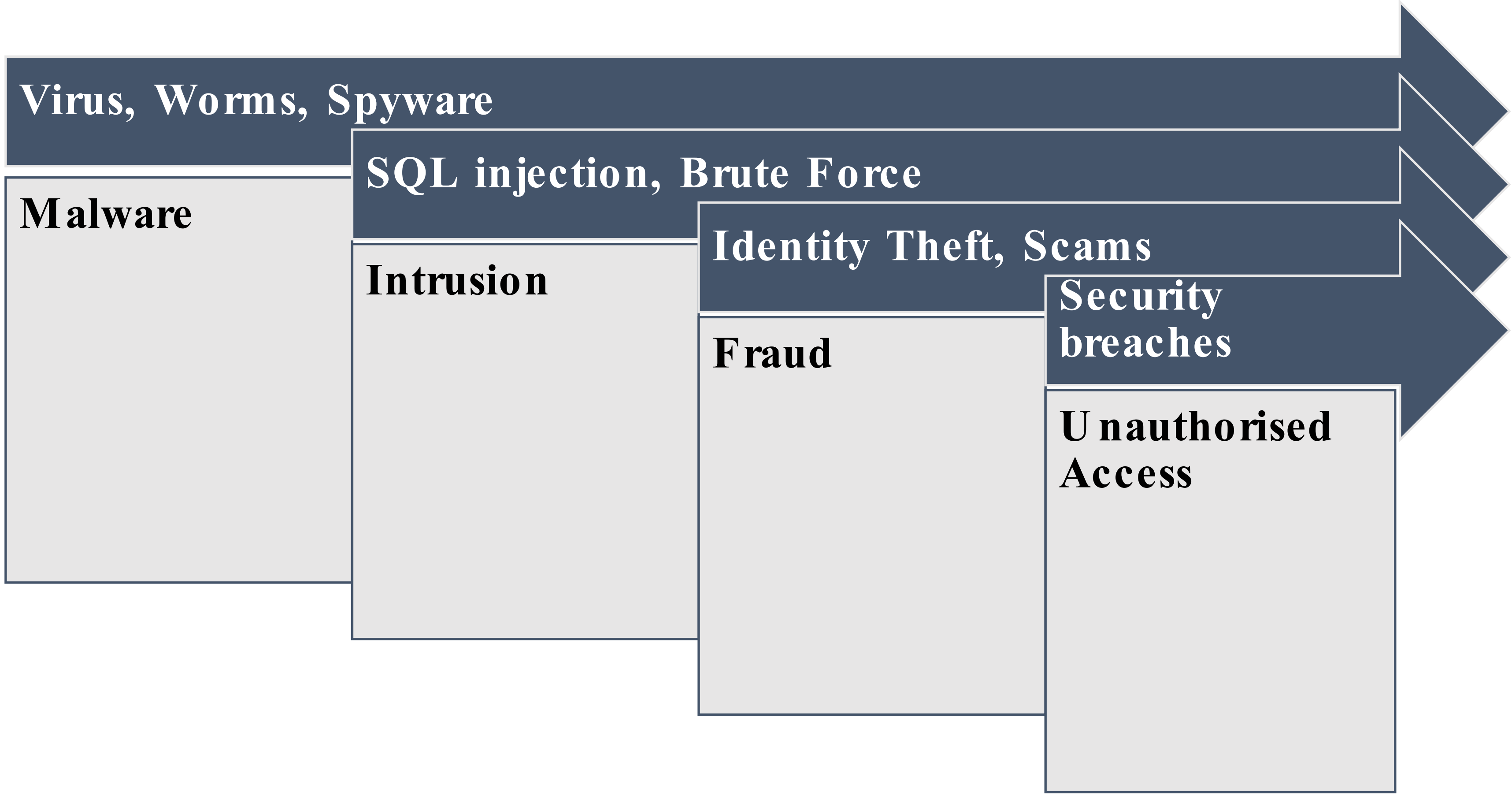
Phase 2: Detection & Analysis

Incident Classification – why incidents need to be classified?

- Not all incidents can be handled in the same way
- Different types of incidents have different response strategies.
- It is therefore important to provide a definitive classification for incidents
- This will be used as a basis for defining more specific handling procedures
- Certain countries have come up with their Incident Classification schema to facilitate their response strategies. Example include Mauritius.

Phase 2: Detection & Analysis

Incident Classification – Examples



Virus, Worms, Spyware

Malware

SQL injection, Brute Force

Intrusion

Identity Theft, Scams

Fraud

Security breaches

Unauthorised Access

Phase 2: Detection & Analysis

Incident Prioritization

An incident is prioritized based on the following aspects:

- The severity level after incident analysis
- The potential danger and urgency for responding the incident
- The functional and information impact of the incident
- The level of investment or resources required to respond to the incident

Phase 2: Detection & Analysis

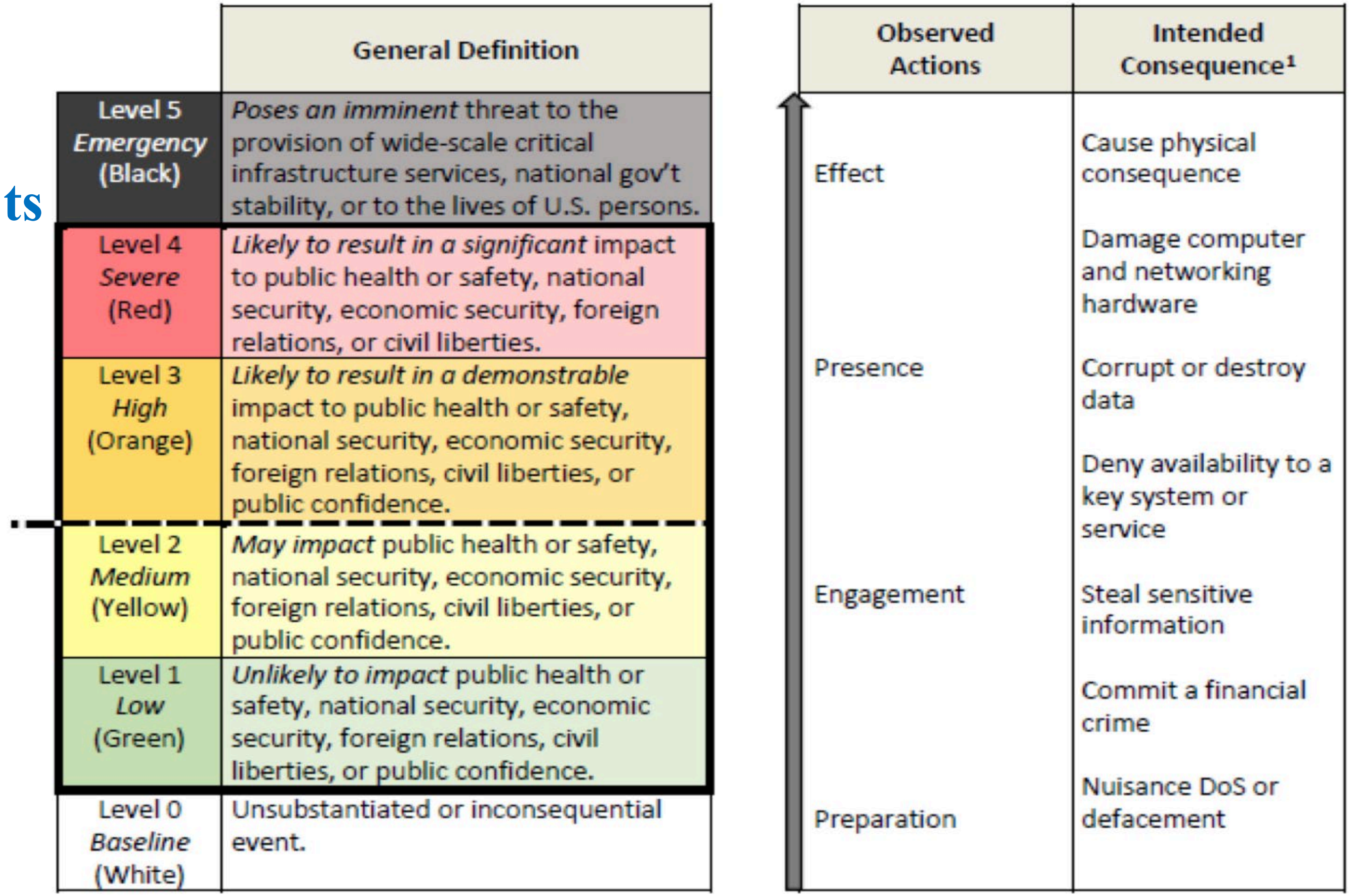
Criteria for determining the Severity Level

- Incidents severity level may be determined based on the following fa

Impact	
Functional	Incidents that may impact the business functionality of a nation Example: DoS attack or Web defacement
Information	Incidents may affect the confidentiality, integrity, and availability of a nation's information Example: malicious attack gathering sensitive information
Recoverability	The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances, it is not possible to recover from an incident

Phase 2: Detection & Analysis

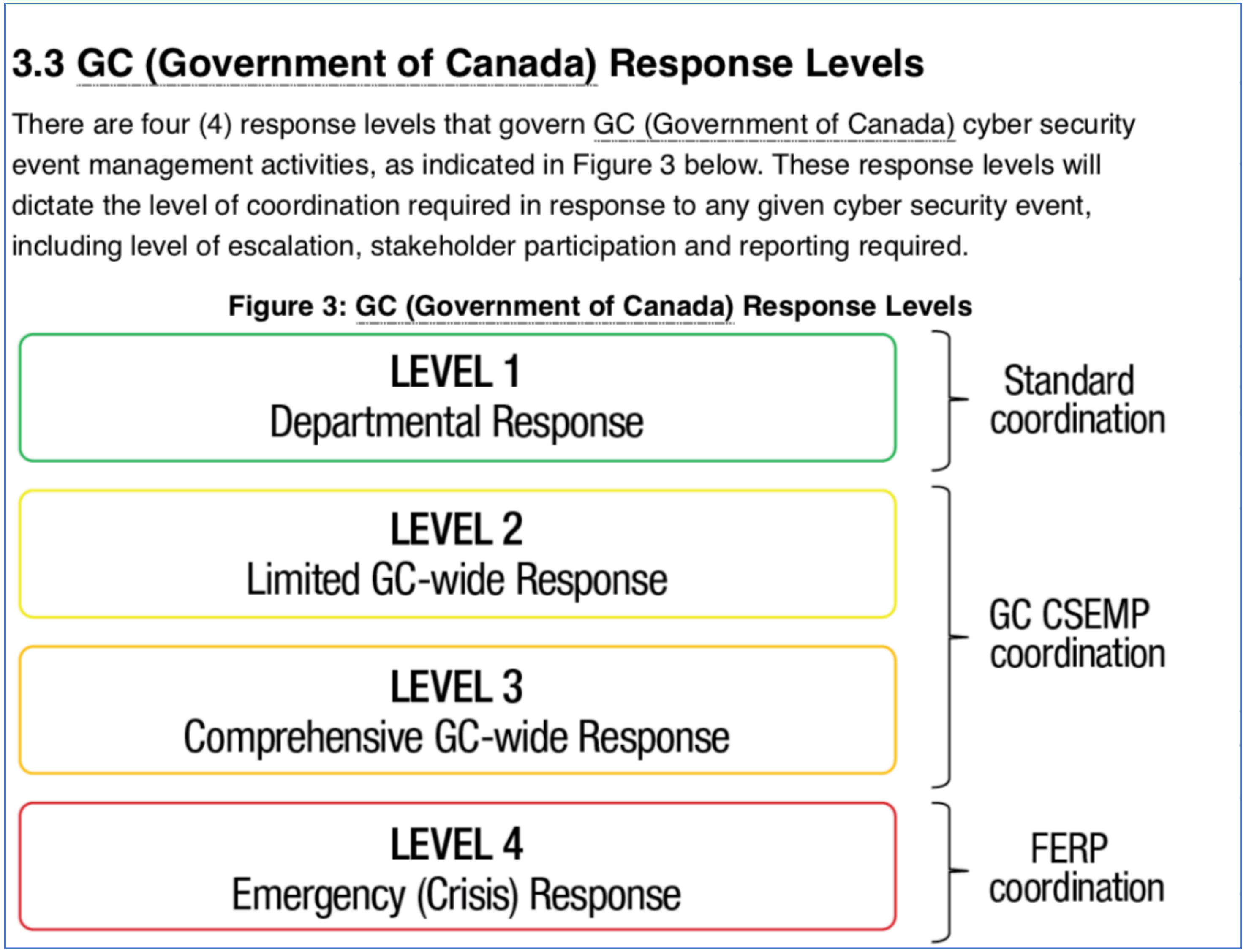
Incident Prioritisation – Severity Levels of Incidents Case Example: USA National Cyber Incident Response Plan



	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

Case Example: Canada



3.3 GC (Government of Canada) Response Levels

There are four (4) response levels that govern GC (Government of Canada) cyber security event management activities, as indicated in Figure 3 below. These response levels will dictate the level of coordination required in response to any given cyber security event, including level of escalation, stakeholder participation and reporting required.

Figure 3: GC (Government of Canada) Response Levels

LEVEL 1
Departmental Response

LEVEL 2
Limited GC-wide Response

LEVEL 3
Comprehensive GC-wide Response

LEVEL 4
Emergency (Crisis) Response

Standard coordination

GC CSEMP coordination

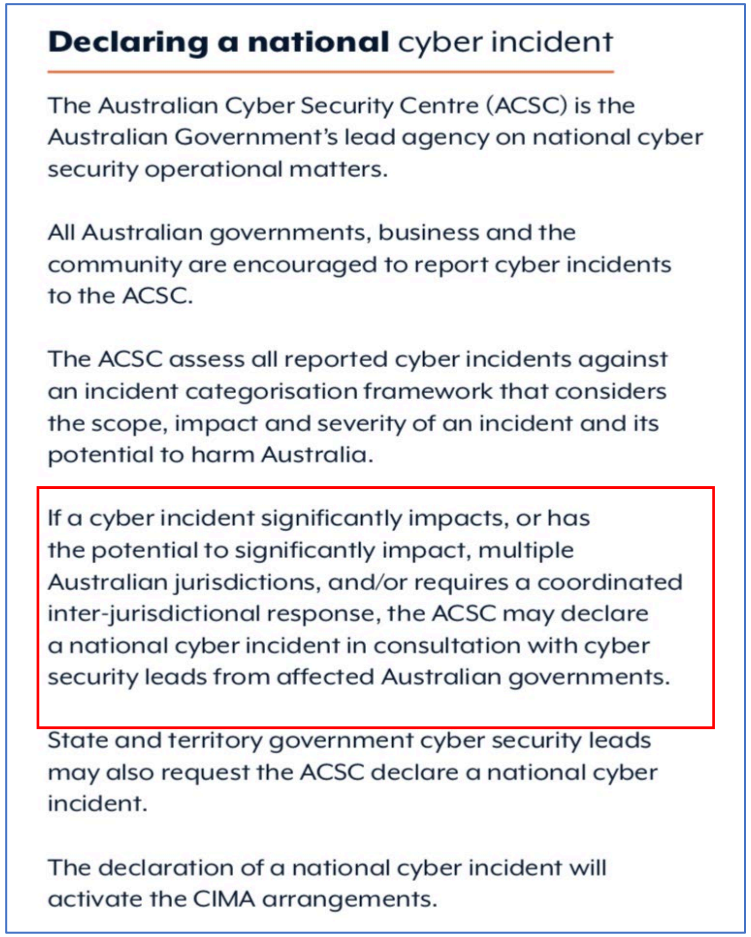
FERP coordination

Declaring a National Cyber Incident

- After the detection and analysis phase, whereby the scope, impact and severity of an incident and its potential harm has been assessed and if:
  - ➢a cyber incident significantly impacts, or has the potential to significantly impact a nation
  - ➢a cyber incident or group of related cyber incidents that together are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the nation or to the public health and safety of a nation
- A national cyber incident may be declared.
- The declaration of a national cyber incident will activate the National Cyber Crisis Management Plan.

Declaring a National Cyber Incident

Case Example – Australia



Declaring a national cyber incident

The Australian Cyber Security Centre (ACSC) is the Australian Government's lead agency on national cyber security operational matters.

All Australian governments, business and the community are encouraged to report cyber incidents to the ACSC.

The ACSC assess all reported cyber incidents against an incident categorisation framework that considers the scope, impact and severity of an incident and its potential to harm Australia.

If a cyber incident significantly impacts, or has the potential to significantly impact, multiple Australian jurisdictions, and/or requires a coordinated inter-jurisdictional response, the ACSC may declare a national cyber incident in consultation with cyber security leads from affected Australian governments.

State and territory government cyber security leads may also request the ACSC declare a national cyber incident.

The declaration of a national cyber incident will activate the CIMA arrangements.

Case Example – Mauritius

A National Cyber Incident is declared if the severity level is High, Very High or Critical.

CERT-MU

Incident Documentation

- After the declaration of an incident, it is very important to document the incident as this will help in the other phases of incident response.
- The incident coordination team should keep track of the following:
  - ➢The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
  - ➢A summary of the incident
  - ➢Indicators related to the incident
  - ➢Actions taken by all incident handlers on this incident
  - ➢Chain of custody, if applicable
  - ➢Impact assessments related to the incident
  - ➢A list of evidence gathered during the incident investigation
  - ➢Comments from incident coordination team

CERT-MU

Information Sharing and Communication

- One of the most important aspect of incident response coordination is information sharing and communication
- The information sharing and communication strategy depends on country to country
- It is very important to devise a strategy that clearly states what can be shared with whom, when and over what channels
- Incident of national significance may be shared to the following parties:
  - ➢Government bodies
  - ➢Law enforcement
  - ➢ISPs
  - ➢Media
  - ➢External parties (international CERTs)
  - ➢Citizens, customers or constituency members

Information Sharing and Communication

Incident of National significance requires the incident coordination team to:

- Deliver coordinated, prompt, reliable, and actionable information to the whole community and the public, as appropriate, through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding significant threat or malicious cyber activity, as well as the actions being taken and the assistance being made available, as appropriate.

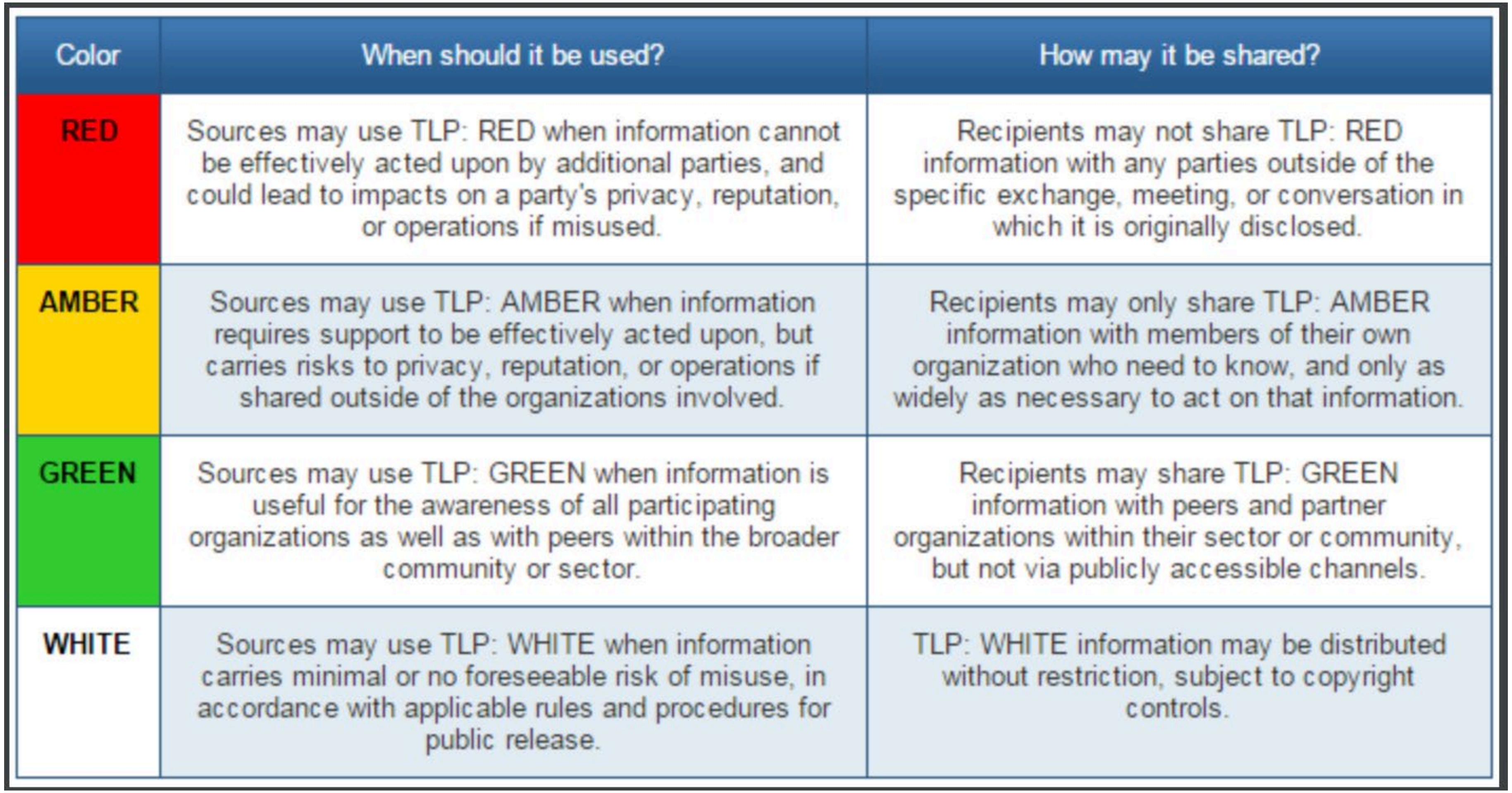
Information Sharing and Communication

Information sharing using Traffic Light Protocol

- The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience.
- It uses four colours to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipients.
- TLP is used by many countries and organisations to share information – e.g include CERT Mauritius, Estonia, USA

Information Sharing and Communication

Information sharing using Traffic Light Protocol (TLP)



Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Phase 3: Containment, Eradication and Recovery

- The purpose this phase is to contain and mitigate the effects of incidents when they occur.
- Activities in this phase will vary depending on the nature of the event, but could include actions such as the installation of patches, implementation of preventative measures, containment and eradication of a confirmed incident (which may involve investigative analysis), the invocation of business continuity and disaster recovery plans or the temporary shutdown of vulnerable services.
- Regardless of the type of event, the end goal of the phase is to minimize impacts and ensure the timely restoration of normal operations.

Phase 3: Containment, Eradication and Recovery

- This phase is the period in which incident response team tries to contain the incident, mitigate the effects and recover from it.
- Containment strategies vary based on the type of incident and may depend on the following:
  - ➢Potential damage
  - ➢The need to preserve evidence
  - ➢Service availability (e.g., network connectivity, services provided to external parties)
  - ➢Time and resources required
  - ➢Effectiveness of the strategy (e.g., partial containment, full containment)
  - ➢Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

Phase 3: Containment, Eradication and Recovery

- After an incident has been contained, eradication may be necessary to eliminate components of the incident such as removal of malicious components, disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited.
- In recovery, systems are restored to normal operation and are confirm that they are functioning normally, and vulnerabilities are remediated to prevent similar incidents
- Eradication and recovery should be done in a phased approach so that remediation steps are prioritized.

Phase 4: Post Incident Activity

- The post-event activity phase leverages knowledge gained from each cyber security event to ensure the continuous improvement of the cyber security incident response and, by extension, the security posture of the nation as a whole.
- The purpose of this phase is to formally closeout the cyber incident by conducting a post-event analysis, identifying lessons learned (when applicable) and driving changes to security policy or enterprise security architecture improvements, as required.

Phase 4: Post Incident Activity

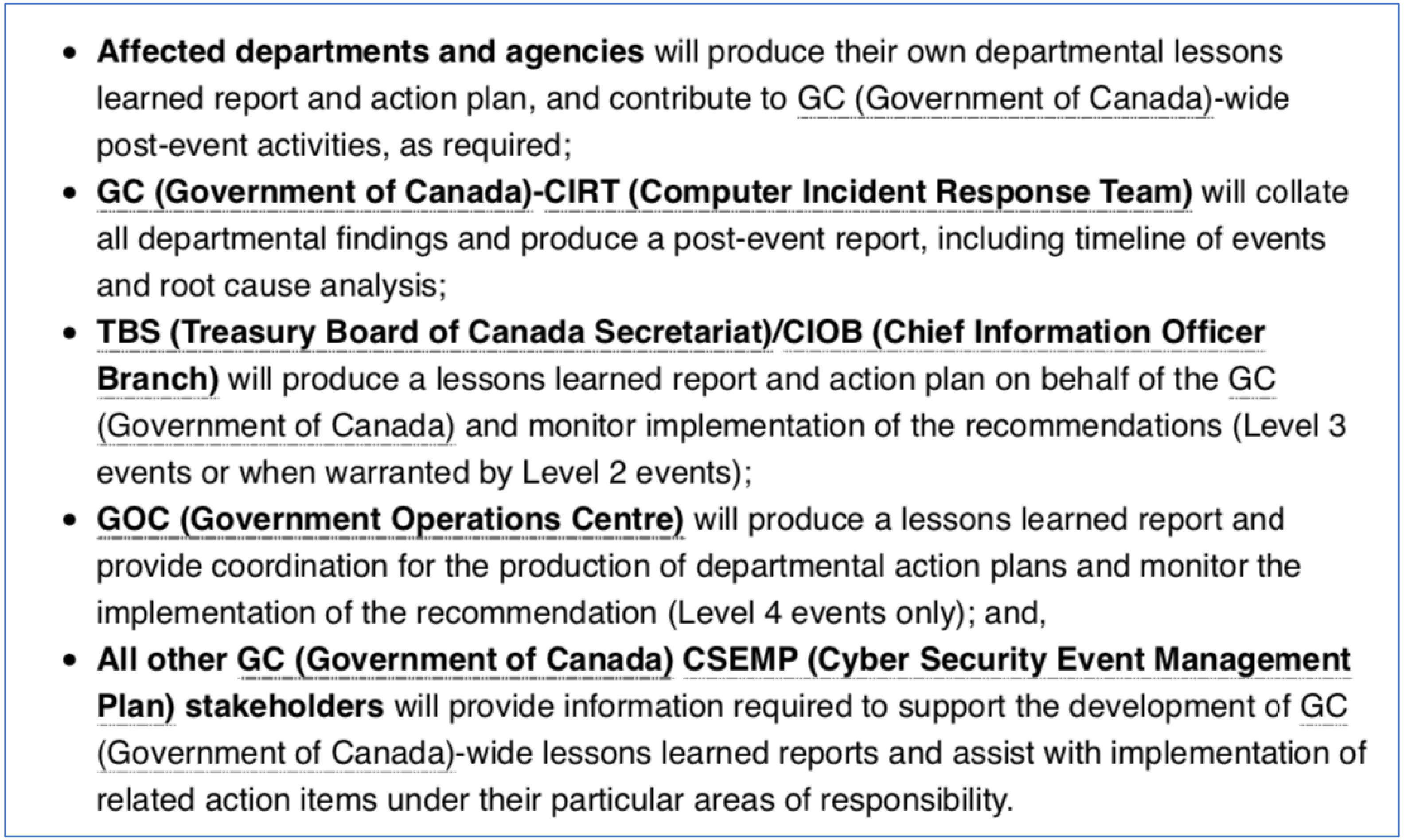
- The post-event activity phase leverages knowledge gained from each cyber security event to ensure the continuous improvement of the cyber security incident response and, by extension, the security posture of the nation as a whole.
- The purpose of this phase is to formally closeout the cyber incident by conducting a post-event analysis, identifying lessons learned (when applicable) and driving changes to security policy or enterprise security architecture improvements, as required.

CERT-MU

Phase 4: Post Incident Activity

Example:
Canada Cyber Security Event Management Plan

Post Incident Activities



- **Affected departments and agencies** will produce their own departmental lessons learned report and action plan, and contribute to GC (Government of Canada)-wide post-event activities, as required;
- **GC (Government of Canada)-CIRT (Computer Incident Response Team)** will collate all departmental findings and produce a post-event report, including timeline of events and root cause analysis;
- **TBS (Treasury Board of Canada Secretariat)/CIOB (Chief Information Officer Branch)** will produce a lessons learned report and action plan on behalf of the GC (Government of Canada) and monitor implementation of the recommendations (Level 3 events or when warranted by Level 2 events);
- **GOC (Government Operations Centre)** will produce a lessons learned report and provide coordination for the production of departmental action plans and monitor the implementation of the recommendation (Level 4 events only); and,
- **All other GC (Government of Canada) CSEMP (Cyber Security Event Management Plan) stakeholders** will provide information required to support the development of GC (Government of Canada)-wide lessons learned reports and assist with implementation of related action items under their particular areas of responsibility.

CERT-MU

Thank You

CONTACT US

Computer Emergency Response Team of Mauritius (CERT-MU)

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