

UNCLASSIFIED

TLP: GREEN



For Public Release

**UNCLASSIFIED // OUO**

**TLP: GREEN**

This page is intentionally left blank



For Public Release

**UNCLASSIFIED // OUO****TLP: GREEN**

Revision	Amendments	Date
1	First release	Month XX, 2019
2	Comments responded to, modified to keep CONOP specific to the 2019 election and not a general partnership. Injury Matrix updated to reflect Playbook version	8 May, 2019
3	Response levels changed to reflect CCCS and Stakeholder roles and responsibilities	15 May, 2019
4	Response levels modified to respect EC comments, Communications team at CCCS and EC added to POCs list	21 May, 2019
5	Injury matrix adjusted (removal of H flags). Slight wording change in 4.1 Roles & Responsibilities for [redacted] Phone numbers added for EC on-call staff	6 June, 2019



For Public Release

**UNCLASSIFIED // OUO****TLP: GREEN**

# TERM OF CONCEPT OF OPERATIONS DOCUMENT

This document comes into effect on the day that it is signed by the Parties and will remain in effect until either Party rescinds this document.

This document may be modified in writing at any time with the written consent of both Parties. Any revisions made after the signing of the document should be documented at the front of this document.

## PRIVACY AND DATA PROTECTION

The Canadian Cyber Centre for Cyber Security (CCCS) is part of the Communications Security Establishment (CSE). Data obtained during the course of cyber event management activities will be considered to be under CSE control if it is relevant (or in the case of private communications, essential) to CSE's mandate as stated in 273.64(1)(b) of the National Defence Act. That data, from which any personal information, as defined under the federal Privacy Act, will first be removed, may be used for the purposes of fulfilling that mandate, and may be shared with domestic and internal partners involved with cyber security, both in the public and private sector. Data that is not relevant to CSE's mandate must be deleted in accordance with CSE's retention schedules.

CSE's activities are subject to rigorous CSE policies and, in case of activities involving possible private communication interceptions, to a ministerial approval detailing the safeguards and protection measure of the data obtained by CSE. CSE activities are subject to federal privacy and access to information legislation, among other applicable legislation, and are subject to review by the CSE Commissioner, the Information Commissioner, the Privacy Commissioner, the Auditor General and any other body established by Parliament for review purposes. Interviews or documentation may be requested as part of a review; Elections Canada (EC) will cooperate fully with any such requests.

For the Communications Security Establishment:

For Elections Canada:



UNCLASSIFIED // OOU

TLP: GREEN

# TABLE OF CONTENTS

- 1 INTRODUCTION .....7
  - 1.1 Purpose .....7
  - 1.2 Audience.....7
  - 1.3 Scope.....7
  - 1.4 Objectives .....8
  - 1.5 Definitions .....8
- 2 CYBER SECURITY EVENT MANAGEMENT .....9
  - 2.1 Preparation .....9
  - 2.2 Detection and Assessment.....10
  - 2.3 Mitigation and Recovery .....10
  - 2.4 Post-Event .....10
- 3 EVENT SURGE .....11
  - 3.1 Surge in Action .....11
- 4 ROLES AND RESPONSIBILITIES .....12
  - 4.1 Preparation .....12
  - 4.2 Detection & Assessment.....12
  - 4.3 Mitigation & Recovery .....13
  - 4.4 Post-Event Activity .....13
- 5 DETERMINING RESPONSE.....14
  - 5.1 Injury Test(S) .....14
  - 5.2 Response Levels .....14
    - 5.2.1 GC-CSEMP Coordination .....14
    - 5.2.2 Level 1: Day-to-Day Operations Within a Department.....14
    - 5.2.3 Level 2: Heightened Attention is Required.....14
    - 5.2.4 Level 3: Immediate Focus and Action is Required.....14
  - Level 4: Severe or Catastrophic Event .....14
- 6 REPORTING AND COMMUNICATION.....15
  - 6.1 Points of Contact .....15
    - 6.1.1 Elections Canada Contacts .....15
    - 6.1.2 Elections Canada Contacts .....15
    - 6.1.3 IBM Contacts .....15
  - 6.2 Notifying Stakeholders.....15
  - 6.3 CCCS Products .....16



**UNCLASSIFIED // OUO**

**TLP: GREEN**

6.3.1 Cyber Alert and Advisories ..... 16

6.3.2 Cyber Flash ..... 16

6.3.3 Incident Notification ..... 16

6.3.4 After Action Report..... 16

## LIST OF ANNEXES

Annex A: Points of Contact ..... 17

Annex B: Injury Tests ..... 19

    B.1 CCCS Injury Test ..... 19

    B.2 EC Injury Test ..... 20

    B.3 EC & CCCS Response Levels ..... 21

Annex C: Glossary ..... 22

Annex D: References ..... 23



UNCLASSIFIED // OUO

TLP: GREEN

## 1 INTRODUCTION

### 1.1 PURPOSE

The Cyber Defence Operations Working Group (CDOWG) is a partnership between the Canadian Centre for Cyber Security (CCCS) and Elections Canada (EC). The purpose of the CDOWG, is to provide an operational framework for cybersecurity information sharing and for the management of cyber security events (including cyber threats, vulnerabilities or security incidents) that impact or threaten to impact the 43<sup>rd</sup> general election scheduled for October 2019.

This Concept of Operations (CONOP) outlines the actions required to ensure that cyber security events are addressed in a consistent, coordinated and timely fashion. The following procedures and policies will be tested and reviewed through simulations and exercises, and modified as required.

### 1.2 AUDIENCE

The intended audience for this document is for any CSE and EC staff involved in the cyber security of the 43<sup>rd</sup> general election scheduled in October 2019.

### 1.3 SCOPE

The scope of this document is limited to cyber security events (including threats, vulnerabilities or security incidents) on EC information systems or systems that engage with EC IT systems that:

- Affect or may affect delivery of election programs and services to Canadians, government operations, security or privacy of information or confidence in government; and
- Require an integrated Government of Canada (GC)-wide response to minimize impacts and enable prompt mitigation and restoration of government programs and services.

*This document does not address:*

- Cyber security events outside the realm of the 43<sup>rd</sup> general election in October 2019;
- Cyber security events coordinated by the Government Operations Centre (GOC);
- The coordination of cross-jurisdictional cyber security events (e.g. provincial, territorial, municipal or international elections); and
- Response activities that lie outside the mandates of either CCCS or EC.

This document shall be reviewed at the request of either Party.



### 1.4 OBJECTIVES

The objectives of the CDOWG CONOP are to:

For Public Release

UNCLASSIFIED // OUO

TLP: GREEN

- Create a working concept of operations to which the CDOWG stakeholders can and will turn to for guidance on when, how, and whom to notify during a cyber incident(s);
- Increase situational awareness of cyber event coordination and management within the CDOWG;
- Formalize and centralize processes by which CCCS and EC will conduct cyber event management; and
- Provide specific contacts for reporting cyber incident(s).

## 1.5 DEFINITIONS<sup>1</sup>

<p><b>Event</b></p>	<p>Any observable occurrence, omission, or situation that may be detrimental to the security of a cyber system, including threats, vulnerabilities, and security incidents.</p>
<p><b>Incident</b></p>	<p>Incidents are a subset of cyber security events. Incidents are any event (or collection of events), act, omission or situation that has resulted in a <i>compromise</i>.</p>
<p><b>Threat</b></p>	<p>An activity <i>intended to compromise</i> the security of an information system by altering the availability, integrity, or confidentiality of a system or information it contains.</p>
<p><b>Vulnerability</b></p>	<p>A factor that could be an accidental or deliberate factor in design or configuration that could <i>increase susceptibility</i> to compromise.</p>

<sup>1</sup> The definitions are taken from the GC CSEMP 2018.



UNCLASSIFIED // OUO

TLP: GREEN

## 2 CYBER SECURITY EVENT MANAGEMENT

The overall cyber security event management process defined in this document has several phases, as outlined in **Figure 1** below. Each phase of this cycle feeds into one another through reporting and communication between stakeholders. Mitigation advice and status updates are shared with both affected and non-affected parties in a timely fashion, enabling situational awareness and supporting informed decision-making.

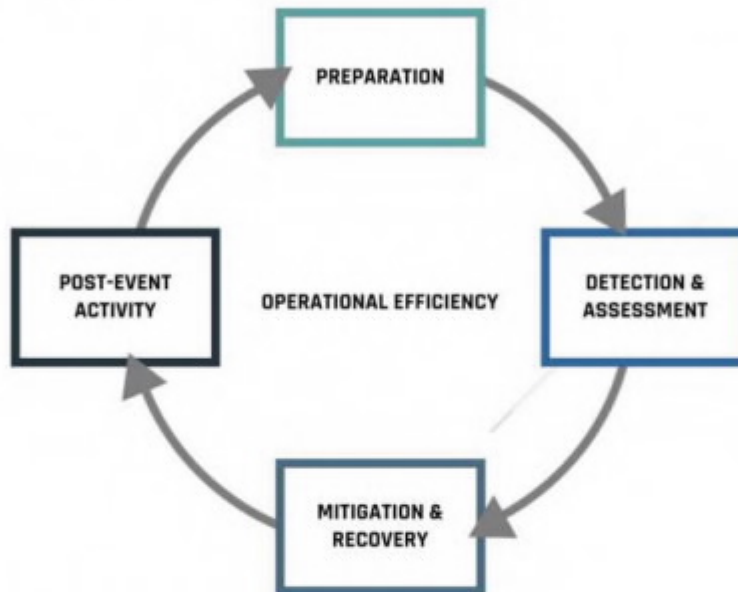


Figure 1: Event Management Lifecycle

### 2.1 PREPARATION

The initial phase, *preparation*, involves planning of general readiness activities when responding to the broad range of cyber security events. Key activities include:

- Understand the scope of the EC IT Ecosystems in support of the 43<sup>rd</sup> general election;
- Assign team leads and provide the points of contact for reporting and communications;
- Provide advice and guidance regarding best practices on protecting EC infrastructure;
- Review and fix vulnerabilities;
- Change control and or other system and services related to emergency services;
- Review and formalize a joint cyber event management plan for EC infrastructure;
- Define roles and responsibilities; and
- Practice incident response plan through exercises, scenarios and tests to validate defence posture and procedures.

UNCLASSIFIED // OUO

TLP: GREEN

## 2.2 DETECTION AND ASSESSMENT

---

The second phase, *detection & assessment*, involves the discovery and monitoring of potential and/or confirmed cyber security incidents. This phase also includes an assessment to determine the scope of response. Key activities to engage in during this phase:

- Look for signs of abnormal network activity through a variety of different sources such as partner reporting, media, or disclosure<sup>2</sup>;
- Gather relevant information, continue monitoring and detection practices, and send reports to the appropriate incident response team;
- Determine, with the help of IT and other professionals, when a cyber security incident has occurred; and
- Determine the level of response and/or if necessary, follow escalation protocols.

## 2.3 MITIGATION AND RECOVERY

---

The third phase, *mitigation & recovery*, consists of all response actions required to minimize impacts to confidentiality, availability and integrity, and to restore normal operations. While specific activities will differ depending on the response assessment, the following are key activities to engage in during this phase:

- Contain (block accounts, websites, services, ports, physical isolation);
- Reduce Impact (how to continue services with the resources left);
- Eradicate (remove malware, patch vulnerabilities, change compromised credentials, etc.); and
- Document (preserve logs, image systems, identify affected computers).

## 2.4 POST-EVENT

---

The final phase, *post-event activity*, is vital for continual improvement of the overall cyber security event management process and, as such, feeds back into the preparation phase to complete the event management life cycle. Key activities within this phase include:

- Review incident response plan;
- Identify lessons learned from the event;
- Improve defensive posture (if possible); and
- Update and enhance incident response plan (if possible).



---

<sup>2</sup> An event can be disclosed through the outlets EC or CCCS has in place such as a hotline, the media, partners, or a dedicated incident inbox.

UNCLASSIFIED // OOU

TLP: GREEN

### 3 EVENT SURGE

For the 43<sup>rd</sup> general election, there will be three operation centres to harmonize analysts' efforts to detect, assess and mitigate election-related incidents promptly.

The surge will consist of three locations: The Edward Drake Building (EDB), [REDACTED] and Elections Canada Headquarters (ECHQ). These coordination centres have been tailored to provide enhanced capabilities to increase operational efficiency.

- **EDB:** EDB will consolidate CSE stakeholders to focus efforts against election-specific threats and decrease response times.
- [REDACTED] Analysts from CCCS, EC, and other partners will collocate and be able to rely on their native systems for easier information sharing and have the ability to work with information and external engagements within a classified space. Reporting will be predominantly unclassified.
- **ECHQ:** EC will provide a location to amalgamate efforts against election-specific threats and decrease response times.

#### 3.1 SURGE IN ACTION

The surge will commence once the writ is issued. Once activated, the surge will operate in four different operational tempos: *one month* before the elections, *one week* before the elections, the *day*<sup>3</sup> of the elections and *one week* after the elections.

The first three surge stages will iteratively increase in tempo while the final stage decreases to standard operational capacity and implements post-event activities. The table below provides the framework to each stage's operational tempo and the resources and activities to be expected.

Table 1: Operational Phases of Surges

Stage	Description	Resources & Activities
Once writ is issued	One month before, reporting will begin through surge communication lines ( <b>Annex A</b> )	<ul style="list-style-type: none"> <li>• Increased distribution of communication products<sup>4</sup></li> <li>• On call analysts</li> <li>• Core hours or as needed</li> </ul>
Two Weeks Before	Elevated coverage with more Duty Analysts deployed to the coordination centres	<ul style="list-style-type: none"> <li>• 24/7 availability and inbox monitoring</li> </ul>
Day of (Polling Day)	Maximum resource deployment will include additional analysts deployed and extended shifts/duty hours to support 24/7 effort	<ul style="list-style-type: none"> <li>• 24/7 on-site monitoring capability to review all network activity provides support to systems and effort</li> </ul>
One Week After	Conduct post-event activities and analysis.	<ul style="list-style-type: none"> <li>• Core hours or as needed</li> </ul>

<sup>3</sup> Day of the elections is scheduled to take place on or before October 21<sup>st</sup> and four hours after polls close.

<sup>4</sup> Examples of communication product types can be found in **Section 6.3**.

For Public Release

UNCLASSIFIED // OOU

TLP: GREEN


## 4 ROLES AND RESPONSIBILITIES

Roles and responsibilities are predominantly shared between the [redacted] section within CCCS and EC IT Security but may diverge to a CCCS [redacted] lead when the threat reaches a level 4 (refer to response levels for more information).

### 4.1 PREPARATION

Task(s)	Lead
Understand the scope of the systems with an impact on the elections	CCCS [redacted] and EC IT Security
Provide advice and guidance regarding best practices on protecting EC infrastructure and if needed provide defence services	CCCS
Address and advise on vulnerabilities	CCCS [redacted] and EC
Using CONOP as guiding principles to develop a cyber event management plan that: <ul style="list-style-type: none"> <li>Establishes the organizational structure for incident response;</li> <li>Defines roles and responsibilities; and</li> <li>Assign team leads and provide the points of contact for reporting and communications.</li> </ul>	CCCS and EC
Practice incident response plans through exercises, scenarios and tests to validate defence posture and procedures	CCCS and EC

### 4.2 DETECTION & ASSESSMENT

Task(s)	Lead
Look for signs of abnormal network activity	CCCS and EC
Notify the appropriate CDOWG stakeholder of potential or confirmed activity (Annex A)	CCCS [redacted] and EC IT Security
Gather relevant information, continue monitoring and detection practices, and relay findings to incident lead and/or partner agencies for awareness	CCCS and EC
If necessary, engage with subject matter experts to determine analytical direction/action regarding cyber security concerns	CCCS [redacted] and EC IT Security
 [redacted] the [redacted] response and [redacted] follow escalation pr [redacted]	CCCS [redacted]
Triage of internal EC incidents and low level threats <ul style="list-style-type: none"> <li>EC employs methodology based on the GC-CSEMP (Annex B.2)</li> </ul>	EC IT Security
Triage of medium and higher incidents and threats <ul style="list-style-type: none"> <li>CCCS's injury model can be found in (Annex B.1)</li> </ul>	CCCS [redacted] and EC IT Security

For Public Release

UNCLASSIFIED // OOU

TLP: GREEN

#### 4.3 MITIGATION & RECOVERY

Task(s)	Lead
Contain (block accounts, websites, services, ports, physical isolation)	CCCS and EC IT
Reduce impact (how to continue services with the resources left)	CCCS [ ] and EC IT
Eradicate (remove malware, patch vulnerabilities, change compromised credentials, etc.)	EC IT
Document (preserve logs, image systems, identify affected computers)	CCCS [ ] and IT Security
Cyber Forensics	CCCS

#### 4.4 POST-EVENT ACTIVITY

Task(s)	Lead
Review incident response plan	CCCS [ ] and EC IT Security
Identify and document lessons learned from the event (i.e. After Action Reports)	CCCS [ ] and IT Security
Improve defensive posture (if possible)	CCCS [ ] and EC IT Security
Update and enhance incident response plan (if possible)	CCCS [ ] and EC IT Security



<sup>5</sup> Although CCCS [ ] was listed as the lead, EC may also conduct an After Action Report internally. Go to **Section 6.3.4** for details on After Action Reports.

UNCLASSIFIED // OOU

TLP: GREEN

## 5 DETERMINING RESPONSE

Responses will be determined based on a variety of factors potentially subject to change including the risk, severity of injury (actual or potential), competing priorities and capabilities. Responses will guide stakeholder engagement, expectations and deliverables. In the event there is a variance regarding the classification of severity, a CCCS [ ] representative and an EC representative may assess the impact of the cyber event using appropriate methodologies from each organization.

### 5.1 INJURY TEST(S)

The injury tests of CCCS (Annex B.1) and EC (Annex B.2) share a common purpose which is to form the basis of assessment by measuring the degree of injury that has occurred or could reasonably be expected to occur due to a compromise.

### 5.2 RESPONSE LEVELS

#### 5.2.1 GC-CSEMP COORDINATION

The Government of Canada Cyber Security Event Management Plan (GC-CSEMP) response levels may differ from CCCS response levels. The GC-CSEMP establishes response levels based on the need for cross-governmental coordination procedures. CCCS establishes response levels based on the potential or actual injury to one or more departments. At a minimum CCCS will follow GC-CSEMP with respect to cross-governmental coordination. There are four response levels that govern the cyber security event management activities of CCCS in support of EC. Below is a summary of the possible response activities for each level.

#### 5.2.2 LEVEL 1: DAY-TO-DAY OPERATIONS WITHIN A DEPARTMENT

A **Level 1** event represents day-to-day operations. At this state, response is managed in accordance with EC standard procedures and communication is coordinated with CCCS [ ] for situational awareness, advice and guidance. CDOWG communications team will also be engaged.

#### 5.2.3 LEVEL 2: HEIGHTENED ATTENTION IS REQUIRED

A **Level 2**, event requires EC and CCCS technical staff be on heightened alert for cyber activity, monitoring risk levels and/or ensuring that any impact or potential impact is contained and mitigated. CCCS [ ] may also provide additional targeted advice to departments and agencies on how to proceed with event response. CDOWG communications team will be engaged.

#### 5.2.4 LEVEL 3: IMMEDIATE FOCUS AND ACTION IS REQUIRED

A **Level 3** event indicates that immediate focus and action is required. Event response is led by EC with CCCS [ ] support. CCCS [ ] may provide ongoing direction and guidance on how to proceed with response. EC management [ ] will be engaged. Additional messaging and [ ] actions may be required.

#### LEVEL 4: SEVERE OR CATASTROPHIC EVENT

A **Level 4** is reserved for severe impact events that affect multiple organizations and/or are challenging to scope or mitigate. Mitigation requires complex or non-standard solutions. CCCS [ ] may provide guidance and direction on how to proceed.

UNCLASSIFIED // OUO

TLP: GREEN

## 6 REPORTING AND COMMUNICATION

Continuous (both routine and ad-hoc) reporting and communication are vital to operational efficiency. CCCS [redacted] is the central point to EC for cyber security event reporting. While minor incidents may be dealt with at the departmental level at EC, the majority of cyber security incidents that may or may not affect EC should still be reported to CCCS [redacted]. The expectation is that: *if in doubt, it is better to over report than under report.*

### 6.1 POINTS OF CONTACT

The points of contact provided in **Annex A** are the distribution channels for which stakeholders can expect to receive incident communication and reporting during this event. When contacting other stakeholders, the expectation is that the primary contact is utilised first and secondary contacts are for off-hours and weekends (unless stated otherwise) or in the event that there may be technical issues with the primary method of contact.

#### 6.1.1 CCCS CONTACTS

EC may contact the following teams at CCCS:

- CSE [redacted] Team provides network defence services in the GC. They are the 24/7 contact and when there is a system failure or EC is experiencing technical difficulties with CCCS installed services.
- CCCS [redacted] is the point of contact for situational awareness or escalation of potential or actual incidents.

#### 6.1.2 ELECTIONS CANADA CONTACTS

CCCS [redacted] or CSE [redacted] Team may contact the following team at Elections Canada:

- EC IT Security; is the contact for CCCS [redacted] and the CSE [redacted] Team for information related to an incident affecting EC or information regarding technical concerns or other cyber related issues needs to be shared.

#### 6.1.3 IBM CONTACTS

EC will be the sole point of contact for IBM unless conditions require otherwise.

### 6.2 NOTIFYING STAKEHOLDERS

When suspicious activity, malware or evidence of compromise is confirmed, CCCS or EC will notify the other using standard incident reporting processes. Communications regarding security incident should be handled in accordance with the [redacted] on the [redacted] of such security incidents and [redacted] structure. [redacted] should also provide a [redacted] security incident and a [redacted] available contextual information (e.g. threat type, vector, first time/repeated incident).

**UNCLASSIFIED // OUO****TLP: GREEN**

## 6.3 CCCS PRODUCTS

---

The following section outlines the expected types and frequencies of communications sent by CCCS which may be required throughout an event's lifecycle.

### 6.3.1 CYBER ALERT AND ADVISORIES

A summary of the event, mitigation actions, and technical indicators sent to EC and/or GC Executives. The timeline to issue will vary depending on the severity of the issue but a standard guideline to be expected is as follows:

- High Severity: Within 8 hours of disclosure;
- Medium Severity: Within 24 hours of disclosure; and
- Low Severity: Within 72 hours of disclosure.

### 6.3.2 CYBER FLASH

Non-public alerts that may contain information gleaned from research, response activities as well as mitigation recommendations about a recently identified cyber threat that affects GC and/or its interests or assets. Recipients would include EC and/or GC Executives as soon as possible.

### 6.3.3 INCIDENT NOTIFICATION

Notifications regarding cyber incidents (suspected or confirmed), once they have been analyzed and authorized for release, should be sent to Elections Canada as soon as possible.

### 6.3.4 AFTER ACTION REPORT

An internal report issued post-event<sup>6</sup> containing a detailed breakdown of key actions, findings and decisions, as well as lessons learned that may be applied for future events. Due to the large scale of elections as a cyber event, portions of these reports may be shared GC-wide and with partners for operational maturity of managing cyber events.



---

<sup>6</sup> Suggested timeline for release is 2 weeks to 3 months depending on event complexity.



UNCLASSIFIED // OUO

TLP: GREEN

# ANNEX A – POINTS OF CONTACT

Secondary Contacts are for off-hours and weekends (unless stated otherwise) or for the event that there may be technical issues with the primary method of contact.


## CCCS CONTACTS

ACTIVITY	TEAM	PRIMARY CONTACT	SECONDARY CONTACT
Defence Services	CSE <input type="text"/>		Phone: 613-991-8762
Cyber Incidents	CCCS <input type="text"/>	Phone: 819-956-3441 After-Hours Support: 613-716-3567	

## ELECTIONS CANADA CONTACTS

ACTIVITY	TEAM	PRIMARY CONTACT	SECONDARY CONTACT
Notification of Cyber Incidents, Technical Concerns and/or Issues	EC IT Security		

## IBM CONTACTS

ACTIVITY	TEAM	PRIMARY CONTACT
 Security Project Executive		
IBM Security DPE		
Security Project Executive		

For Public Release

**UNCLASSIFIED // OUO****TLP: GREEN**

ACTIVITY	TEAM	PRIMARY CONTACT
CCCS Communications		
EC Communications	Nick Gamache	Email: <a href="mailto:Nick.gamache@elections.ca">Nick.gamache@elections.ca</a> Phone: 343-548-9061

### COMMUNICATIONS CONTACTS



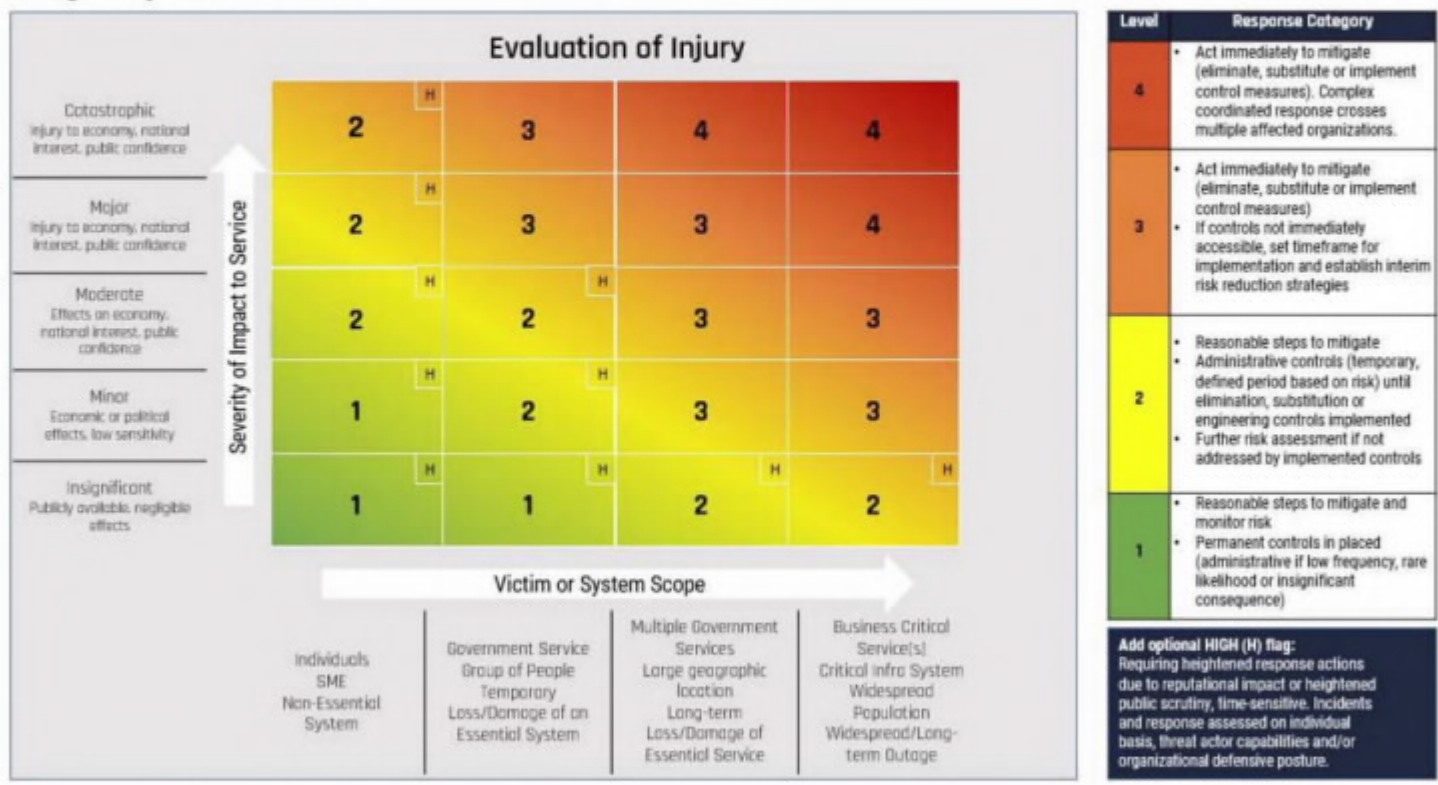
UNCLASSIFIED // OOU

TLP: GREEN

# ANNEX B – INJURY TESTS

## ANNEX B.1 – CCCS INJURY TEST

### Injury Matrix:



For Public Release



UNCLASSIFIED // O/U

TLP: GREEN

## ANNEX B.2 – EC INJURY TEST

		Scope		
		Narrow	Medium	Wide
Severity	Severe	Medium	High	Very High
	Serious	Low	Medium	High
	Limited	Low	Low	Medium
Departmental Impact Level		[Injury Test Result]		

Retrieved from GC-CSEMP: Annex B

For Public Release



UNCLASSIFIED // OOU

TLP: GREEN

# ANNEX B.3 – RESPONSE LEVELS FOR EC & CCCS

The CDOWG CONOP will utilize response levels once an incident has occurred. The table demonstrates the level of response that may be required when an incident has occurred. If there is no incident, there is no need to respond.

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
<b>EC RESPONSE</b>	<p>Low Impact /Low Risk - Director-level led</p> <p>An event of short duration that is not likely to adversely impact or threaten life, health or compromise assets and information. The incident is controlled using the capabilities of a specific department and in accordance with EC emergency response plans</p>	<p>Medium Impact/Medium Risk -Director-General or DCEO level led</p> <p>An unplanned event that may adversely impact or threaten life, health or property, or compromise EC assets and information. The capabilities to manage the event and its may require horizontal and outside agency's assistance</p>	<p>High Impact/High Risk - Corporate level led</p> <p>A serious incident or unplanned event of unpredictable duration that adversely impacts or threatens life, health or property, or compromise EC assets and information on a large scale. Outside emergency personnel, specialist, and horizontal coordination will be required. Long-term implications are expected</p>	<p>EC does not escalate to a level 4 response within their department. At this point, response would be fully coordinated by CCCS for advice, guidance and mitigation strategies</p>
<b>CCCS RESPONSE</b>	<p>Organizations may provide information to the CCCS to identify broader patterns of activities, to inform trends and to request advice and guidance. CCCS ensures that advice and guidance are provided as requested in order to mitigate threat and prevent re-occurrence of event</p>	<p>Declaration authority at this level and above lies with <input type="text"/></p> <p>CCCS may provide additional targeted advice to organizations on how to proceed with event response. CCCS may provide recommendation for the implementation of temporary controls to mitigate the risk</p>	<p>CCCS provides full coordination services and ongoing direction on how to proceed with event response. The implementation of administrative controls are coordinated with stakeholders. Threat has potential to be mitigated/contained if controls are immediately accessible. Stakeholders provide CCCS with ongoing feedback for verification and status updates</p>	<p>CCCS provides full coordination services including eliminating, substituting and implementing control measures in affected organizations. The ability to identify the event scope and coordinate efforts to stop extent of compromise may be limited. Complex coordinated response crosses multiple affected organizations. CCCS will define required controls to mitigate risk levels where possible and analyze of new sources of information</p>



For Public Release

UNCLASSIFIED // OUO

TLP: GREEN

## ANNEX C- GLOSSARY

Term	Definition
CCCS	Canadian Centre for Cyber Security
CDOWG	Cyber Defence Operations Working Group
CIA	Confidentiality, Integrity and/or Availability
CONOP	Concept of Operations
CSE	Communications Security Establishment
EC	Elections Canada
IT	Information Technology
FERP	Federal Emergency Response Plan
GC	Government of Canada
GC CSEMP	Government of Canada Cyber Security Event Management Plan
GOC	Government Operations Centre (GOC)
GE	General Elections



For Public Release

UNCLASSIFIED // OUO

TLP: GREEN

## ANNEX D – REFERENCES

Definition
Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018 from Treasury Board of Canada Secretariat, January 26, 2018.
Concept of Operations (CONOP) Cyber Defence Services at Elections Canada from Communications Security Establishment, August 1, 2018.
Operational Security Standard: Management of Information Technology Security (MITS) from Treasury Board of Canada Secretariat, May 31, 2004.
Elections Canada CEHOM IBM MSSD: Communication Plan from IBM Security, November 27, 2018.

