Elections Canada Security Steering Committee (EC-SSC)

Agenda / January 28, 2021

Elections Canada Security Steering Committee (EC-SSC)

Agenda

Meeting January 28, 2021

MS Teams

Agenda

1. Words of Welcome – 5 mins (Serge)

2. Business Continuity Plan, GE44

3. Security Intelligence

4. Roundtable – 15 mins (all)

5. Adjournment

Elections Canada

GE 44 Incident Management – Business Continuity

For discussion

18/01/2021

elections.ca

Objectives

The two objectives of this presentation are to:

- Validate the GE44 Critical Service List
- Obtain guidance in the Incident Management Framework as it pertains to Business Continuity Planning (BCP) in the pandemic and remote working context.

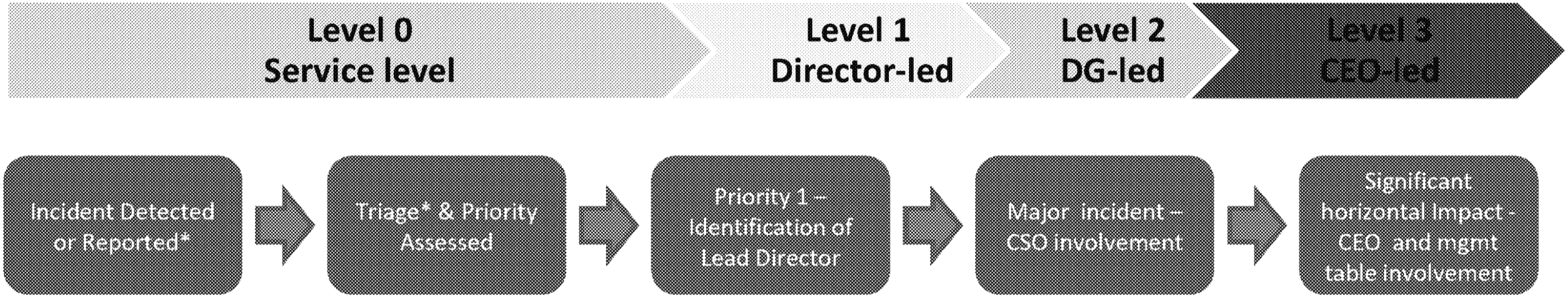
🎯 Slide is unchanged from previous BCP presentations

▲ Slide contains new information

Note: The planning activities leading to the development of incident management and response plans are out of scope of this presentation.

Incident Response Framework

- Incident Response Framework Principles:
  - **All Hazard Approach** – highly adaptable and agile
  - **Risk Based** – Incidents are assessed as to urgency and impact
  - **Coordinated –** *Response is respecting TBS and public health guidance* and coordinated across business lines while respecting operational authorities
- Incidents are managed based on risk level



Level 0
Service level

Level 1
Director-led

Level 2
DG-led

Level 3
CEO-led

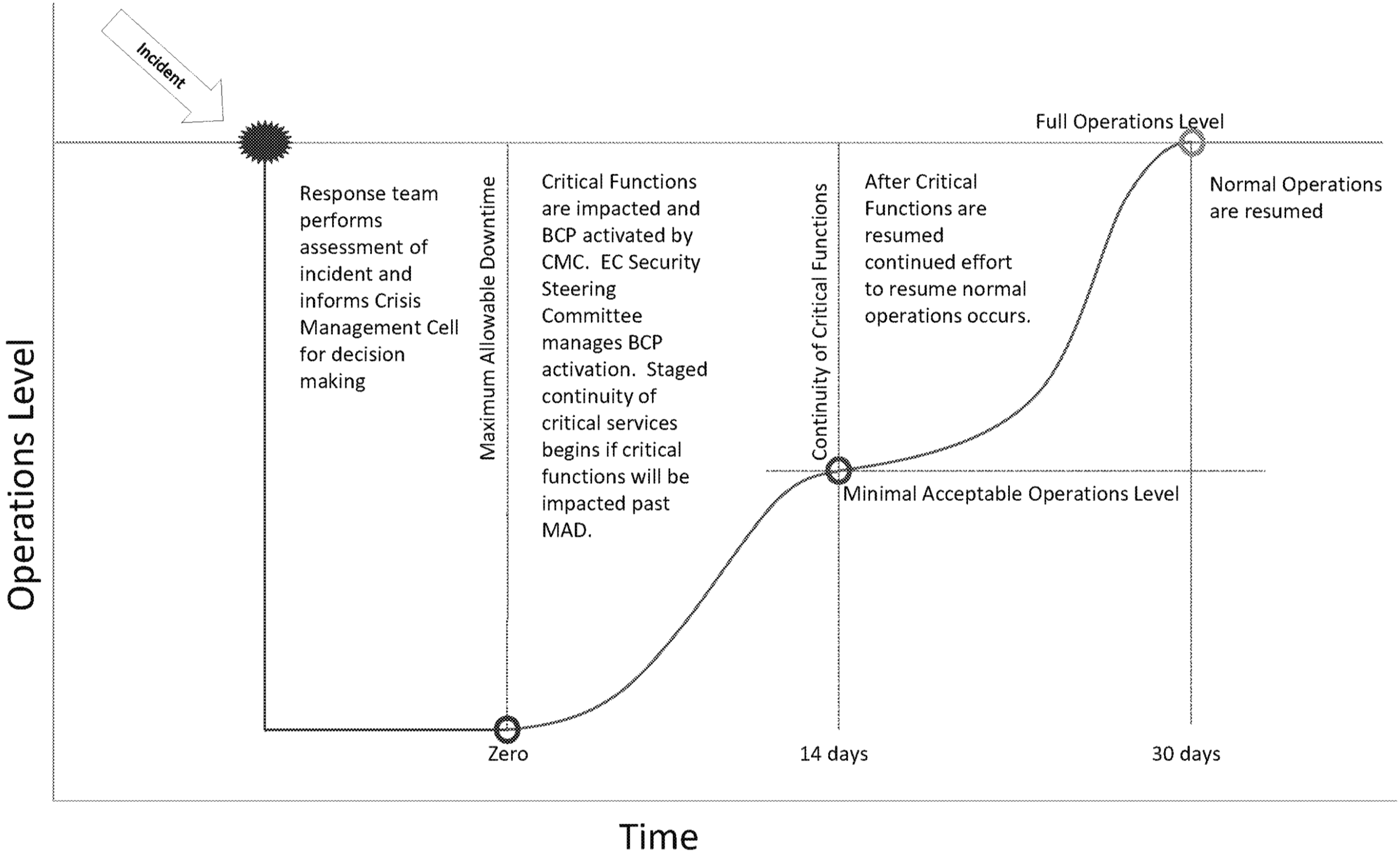
Incident Detected or Reported* → Triage* & Priority Assessed → Priority 1 – Identification of Lead Director → Major incident – CSO involvement → Significant horizontal Impact - CEO and mgmt table involvement

- Incidents are usually detected or reported to a specific functional unit, who is responsible to conduct the triage.
- In the case of more complex incident during a general election, the Integrated *Situational Awareness Coordination Task Force* (ISAC) could be used to identify proper lead functional unit.
- During GE, ISAC would be kept informed of major incidents.

Incident Management Roles - BCP

- Building Emergency Organization (BEO)
  - Coordinates evacuations, shelter in place or lockdown incidents.
  - Coordinates the assessment of service outage.
  - Liaises with Crisis Management Cell to get direction.
- Crisis Management Cell (CMC)
  - CEO, DCEO’s, PACE
  - Determine need to activate Business Continuity Plans, close building, etc.
- Security Steering Committee (SSC)
  - Chaired by DCEO – DT
  - Coordinates BCP activation (prioritized based on Electoral Calendar and operational needs)
- BCP Activation Team (BAT)
  - Under the direction of Director, Enterprise Security
  - Supporting activities (Facilities, IT Ops, Security, HR, PCS and Communications) I
  - Coordinates operational requirements such as alternate sites, additional staff, security and IT services, and develops a communications strategy.
- Integrated Situational Awareness Coordinated Task Force – (ISAC)
  - Kept updated of any BCP activation activities

Incident Response – BCP Activation


Incident
Full Operations Level
Maximum Allowable Downtime
Continuity of Critical Functions
Minimal Acceptable Operations Level
Operations Level
Time
Zero
14 days
30 days

Response team performs assessment of incident and informs Crisis Management Cell for decision making

Critical Functions are impacted and BCP activated by CMC. EC Security Steering Committee manages BCP activation. Staged continuity of critical services begins if critical functions will be impacted past MAD.

After Critical Functions are resumed continued effort to resume normal operations occurs.

Normal Operations are resumed

GE44 Critical Services (for validation)

Business Functions	Pre GE	GE	Post GE	Non-GE
Tier 1 0-24 hours	■	■	■	■
Translation and Publication Services	■	■	▒	▓
2.1 Geography	■	■	▒	▓
3.4 Field Training (All workers)	■	■	▒	▓
4.1 RO & AARO Offices	■	■	▒	▓
4.2 Polling places	■	■	▒	▓
4.5 Field Comms and Support	■	■	░	▓
5.1 Voter Lists and VICs	■	■	░	▓
5.2 One Stop Service Model	■	■	■	▓
5.3 Candidate Services and Support	■	▒	▒	▓
5.4a Regular Voting Services	■	▒	▒	▓
5.4b Special Voting Services	■	▒	▒	▓
5.5 Special Voting Rules (SVR/SVRA)	■	▒	▓	▓
5.6 Election Results	▓	■	■	▓
6.1 Field Locations Technology	■	░	▓	▓
6.2 Telephony Services	■	░	▓	▓
6.3 Hosting Services	■	░	▓	▓
6.6 IT / IM Service Desk	■	■	▒	▓
7.1 Media Relations / Issues Management	■	■	▒	▓
7.2 GE Web Site	■	■	▓	▓
7.3 Public Enquiries	■	■	▒	▓
7.5 Social Media	■	■	▒	▓
8.1 Monitoring / Detecting Electoral Integrity	░	■	▒	▓
8.2 Complaints Management	░	■	▒	▓
8.4 Political Financing - Candidate and Official Agent Support	■	▒	▓	▓

Business Functions	Pre GE	GE	Post GE	Non-GE
Tier 1 0-24 hours - Supporting BCP Activation				
1.1 Internal Communications	▒	▒	▒	▒
1.4 Human Resources - BCP Activation	▒	▒	▒	▒
1.4 Human Resources - GE related activities	▒	▒	▓	▓
1.8 Enterprise Security	▒	▒	▒	▒
1.9 Facilities and Accommodations	▒	▒	▒	▒
Tier 2 24-48 hours	▒	▒	▒	▒
1.2 Election Reporting	▒	▒	▒	▓
1.5 Procurement and Contracting Services	▒	▒	▓	▓
1.10 Legal Services	▒	▒	▓	▓
2.2 Register of Electors	▒	▒	▒	▓
2.3 E-Reg	▒	▒	▓	▓
3.3 Electoral Workers (Recruitment)	▒	▓	▓	▓
3.6 AC and SPS training	▒	▓	▓	▓
4.3 Field Materials	▒	░	▓	▓
4.4 Election Operations Reporting	▒	▒	▓	▓
7.4 Voter Information Campaign	■	■	▓	▓
8.3 Political Financing Election Returns	▓	▒	▒	▓
Tier 3 3-14 days	░	░	░	░
1.3 Field Accounting and Payroll	░	░	▓	▓
5.8 Local Outreach	░	▓	▓	▓
7.6 National Outreach	░	░	░	▓
7.6 Political Financing Return Publication	▓	▓	░	▓
Non-Critical 14+ Days	▓	▓	▓	▓
1.6 Election Budget Management	▓	▓	▓	▓
1.7 GE Public Opinion Research	▓	▓	▓	▓
3.1 Returning Officers (Recruitment)	▓	▓	▓	▓
3.2 Field Liaison Officers (Recruitment)	▓	▓	▓	▓
3.5 Field Engagement	▓	▓	▓	▓
7.7 Civic Education - pre voter	▓	▓	▓	▓

Incident Management – Remote Working

- Remote working means incident management now must account for a decentralized workforce remotely providing for critical service delivery.

Impact	Mitigation	Coordination
Localized Loss of Remote Work Capabilities (Level 1)	Critical staff provided with flex space at ECHQ buildings. – All critical staff accommodated	Business Continuity Activation Team (led by security services) will coordinate available flex space at ECHQ buildings in collaboration with facilities.
Clustered Loss of Remote Work Capabilities (Level 2)	Critical staff will be prioritized prior to being provided flex space at ECHQ building. – Most critical staff accommodated, all critical services expected to meet minimum service level.	Crisis Management Team will be provided impact details by Business Continuity Activation Team to determine which critical staff get prioritized flex space.
Widespread Loss of Remote Work Capabilities (Level 3)	Critical staff will be prioritized prior to being provided flex space at ECHQ building. – Critical staff accommodated on a rotational basis with most critical services meeting minimum service level.	Crisis Management Team will be provided impact details by Business Continuity Activation Team to determine which critical staff get prioritized flex space and to develop a rotation schedule to reduce widespread impact to minimum service levels

GUIDANCE

- Seeking validation of Critical Services
  - Any changes to current ratings
  - Any additional critical services
  - Any critical services are no longer included

- Seeking guidance on proposed process for managing incidents impacting persons working remotely
  - Use of 30 Victoria as flexible workspace on a rotational basis as required in event of outages
  - Validating process for crisis management team meeting remotely

ANNEXES

EC Response Levels

Level 0 - Very Low Risk - Manager Led – Business as Usual

Level 1 – Low Risk – Director led

Short duration incident, not likely to adversely impact health or compromise assets and information. External assistance is not required. DG kept informed.

Examples: malware affecting a few users, localized building incident, incident with a staff.

Level 2 – Medium Risk – DG or DCEO led

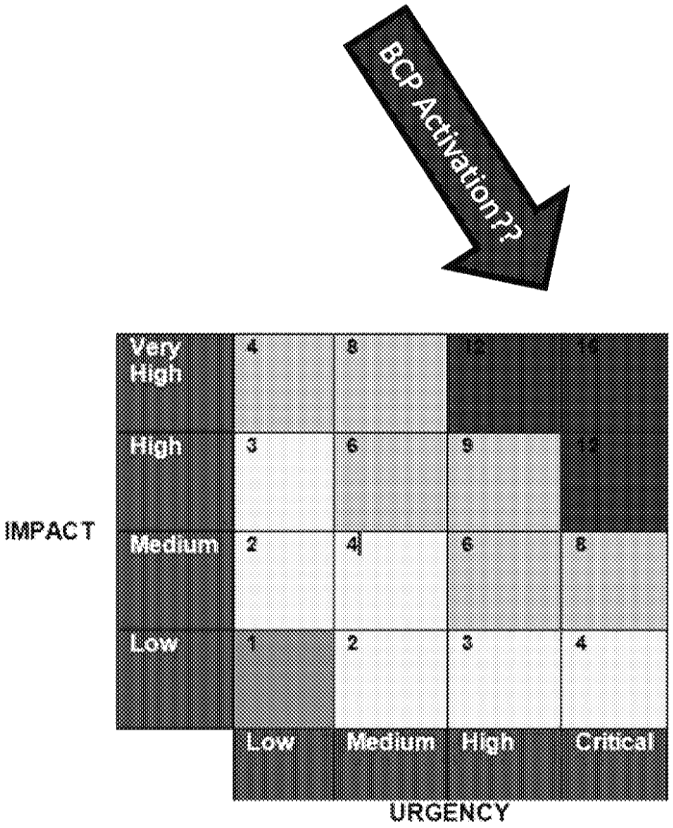
Medium duration event that may adversely impact or threaten life, health, property, or compromise EC assets and information. External assistance may be required. CEO and EC SSC kept informed

Examples: localized multi-floor building flood, contained large scale malware propagation, outside security event affecting EC operations, unreliable threats, security incident in a region affecting operations

Level 3 –Risk – CEO led assisted by EC SSC

A serious 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, specialists, and horizontal coordination will be required. Long-term implications are expected. EXCOM kept informed.

Examples: Fire, Bomb Threat, Building closure, Website defacement, Distributed Denial of Service



BCP Activation??

IMPACT

Very High	4	8	12	16
High	3	6	9	12
Medium	2	4	6	8
Low	1	2	3	4
	Low	Medium	High	Critical

URGENCY

Situational Awareness – SICC

- During Incidents, the **Security Incident Coordination Centre** will coordinate situational awareness products and maintain a single point of contact for recovery activities.

- Communications will be concise emails focused on timely and essential information sharing.

EMAIL TITLE: *Incident Number* – INCIDENT: *small description – Initial or Update #*

  - ***ITSEC190401-01 – INCIDENT: Suspicious behaviour on ecvpn.001.001 – Initial***

Date and Time of Report:: eg. *1 April 2019 – 08:45*

Incident Number: *GroupYYMMDD-ser (eg. ITSECYYMMDD-ser, SECYYMMDD-ser, FACYYMMDD-ser)*

Type of incident: *IT Security / Security / Facility / IT Outage*

Elections Canada Response level : 0 – Notification /*1 – Director-level response / 2 – DG-level response / 3 – Corporate-Level response*

IT Service Priority: *1 – High priority / 2 – Medium severity / 3- Routine*

Responsible Organization: *name of responsible incident manager*

Incident Response Manager: *name of the person managing the initial response*

Responsible Director: name of the Director responsible for service

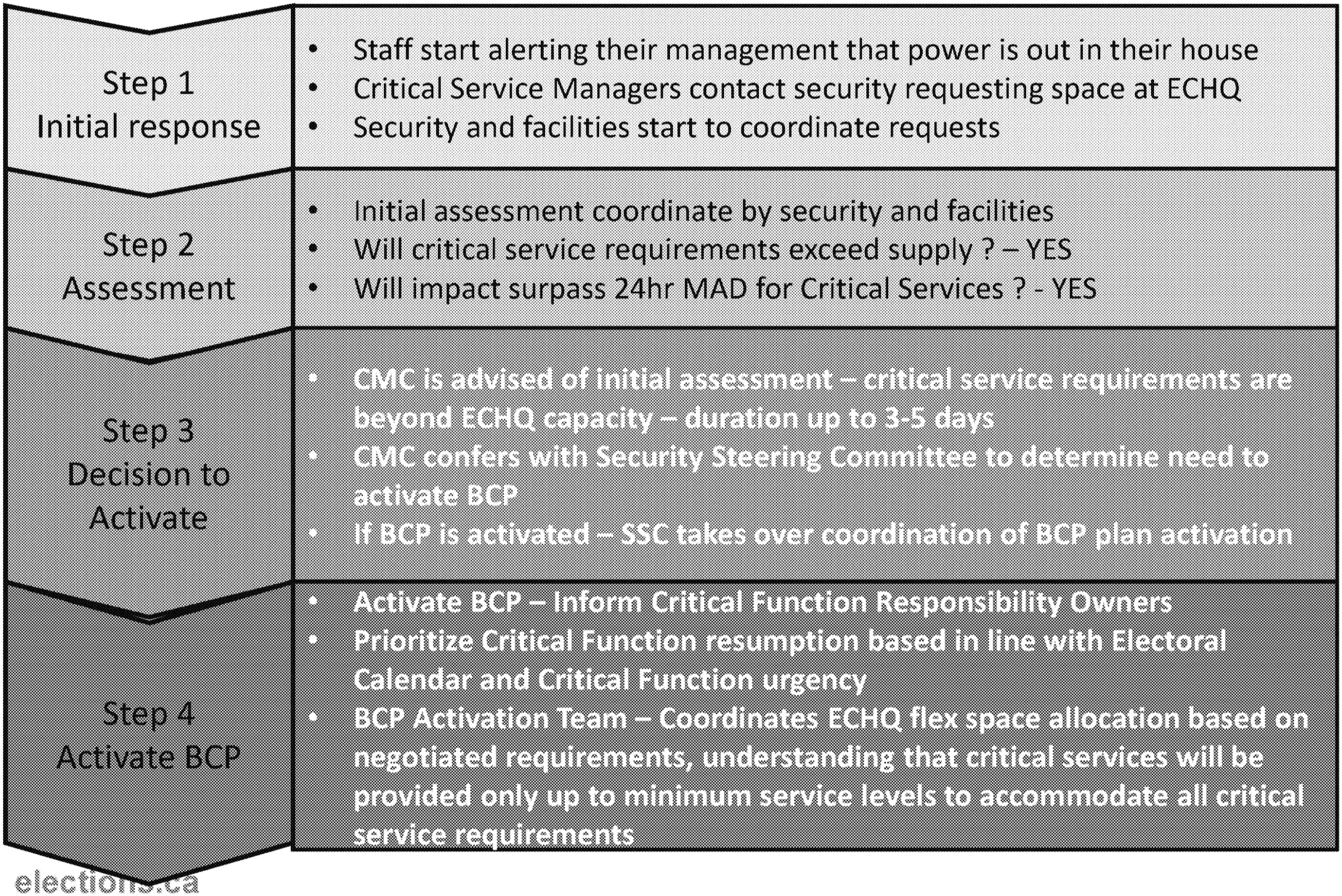
Incident Description: *short description of the incident*

What If …Scenario 1 - Clustered Remote Work Outage

Scenario: Hydro Ontario suffers infrastructure damage resulting in clustered power outages throughout the Ottawa region. Many employees are without power at home and internet services are seriously impacted. While power will be restored intermittently, reliable internet for homeowners may be impacted for 3-5 days. Approximately 300 employees providing critical services are impacted.

- Step 1 – Incident Management
- Step 2 –Determine extent of impact and estimated duration of outage
- Step 3 – MADA – Meet – Assess – Decide - Activate
- Step 4 – Initiate BCP Activation

Incident Response – Scenario 1



Step 1
Initial response

- Staff start alerting their management that power is out in their house
- Critical Service Managers contact security requesting space at ECHQ
- Security and facilities start to coordinate requests

Step 2
Assessment

- Initial assessment coordinate by security and facilities
- Will critical service requirements exceed supply ? – YES
- Will impact surpass 24hr MAD for Critical Services ? - YES

Step 3
Decision to
Activate

- CMC is advised of initial assessment – critical service requirements are beyond ECHQ capacity – duration up to 3-5 days
- CMC confers with Security Steering Committee to determine need to activate BCP
- If BCP is activated – SSC takes over coordination of BCP plan activation

Step 4
Activate BCP

- Activate BCP – Inform Critical Function Responsibility Owners
- Prioritize Critical Function resumption based in line with Electoral Calendar and Critical Function urgency
- BCP Activation Team – Coordinates ECHQ flex space allocation based on negotiated requirements, understanding that critical services will be provided only up to minimum service levels to accommodate all critical service requirements

Elections Canada

Security Intelligence

Program overview

Objectives

- Socialize EC Security Intelligence Program
- Seek guidance for engagement and product distribution

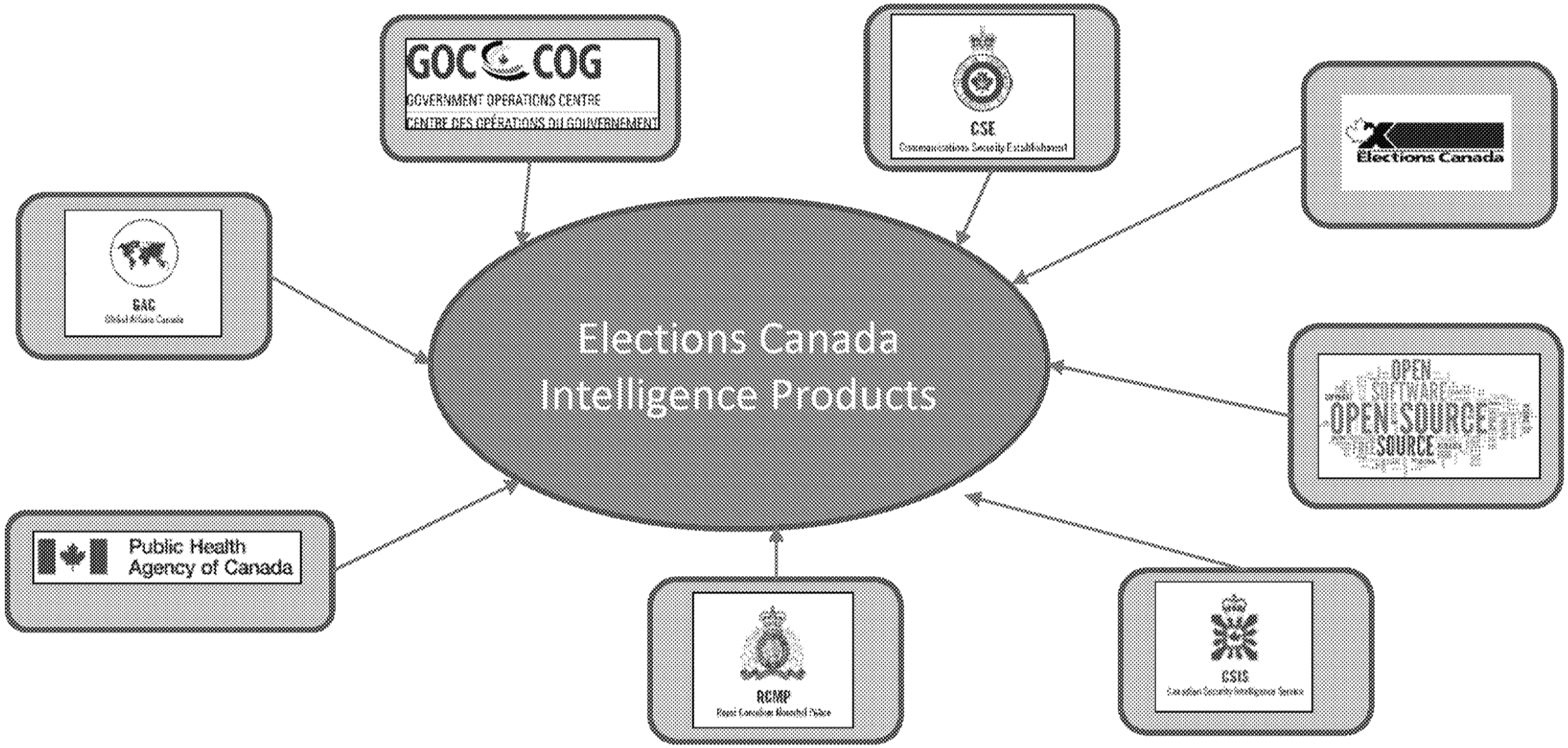
Benefits of Intelligence

- Intelligence is:
  - **Predictive** – Must provide insight and inform
  - **All Source** – Multiple sources for information
  - **Multidisciplinary** – Diverse and various sources
  - **Flexible** – Adaptability to meet unexpected challenges

- Intelligence benefits:
  - Increases EC's security posture
  - Informs decision making to anticipate issues before they arise and prevent emergencies
  - Allows for timely detection, reporting and response when incidents occur

Data Collection

- Information comes in from EC stakeholder, many GC authoritative sources and open sources
- Security Intelligence analysts review and build security intelligence products focused on impacts to EC security posture
- Some authoritative reports and products are shared with stakeholders to support further operational analysis, decision making and situational awareness



Elections Canada Intelligence Products

GOC COG
GOVERNMENT OPERATIONS CENTRE
CENTRE DES OPÉRATIONS DU GOUVERNEMENT
CSE
Communications Security Establishment
Elections Canada
GAC
Global Affairs Canada
OPEN SOFTWARE
OPEN SOURCE
SOURCE
Public Health Agency of Canada
RCMP
Royal Canadian Mounted Police
CSIS
Canadian Security Intelligence Service

External Data Collection

AGENCY	MANDATE / ROLE	ACTIVITIES
GOC COG GOVERNMENT OPERATIONS CENTRE CENTRE DES OPÉRATIONS DU GOUVERNEMENT	• Federal Emergency Management Agency • Coordination of information between departments and agencies	• Monitoring of natural hazards / response to natural disasters. • Support to planning and intergovernmental liaison
CSE Communications Security Establishment	• Information Technology Security • Foreign Intelligence • Supporting CSIS / RCMP	• Intelligence Cyber Assessments • Protect Gov't systems • Provide cyber security advice
CSIS Canadian Security Intelligence Service	• Intelligence and Threat Reduction • Intelligence Assessments	• Threat briefs • Assess hostile state activity
GAC Global Affairs Canada	• G7 Rapid Response Mechanism	• Research on disinformation campaigns • Report global trends • Attribute incidents
RCMP Royal Canadian Mounted Police	• Detect / prevent national security criminal threats in Canada. • Investigate criminal offenses • Key investigative body	• Investigate criminal activity related to interference of Canada's electoral process.
Public Health Agency of Canada	• Emergency preparedness and response, and infectious and chronic disease control and prevention	• Preventing disease and injuries, promoting good physical and mental health, and providing information to support informed decision making.
OPEN SOURCE	• Not Applicable	• Trained analysts gather open source information, and assess it's quality and relevance for use in products

Types of Intelligence Products

Product Type	Value/Purpose	Objective
All Hazards Electoral District Analyses	• To quickly provide information during events (e.g. leveraged heavily during 2019 snow storm)	• To anticipate issues before they arise • Prevent emergencies • Allow for more informed timely responses when emergencies do occur
Single Page Electoral District Summary	• To provide broad information to field personnel • To create a two way relationship where intelligence also flows from the field to the intelligence team	• To provide more targeted scrutiny of potential security issues in the field • Allow for timely detection and reporting by field personnel
Security Information/Event Analyses	• To summarize large security and intelligence related reports or events (e.g. the Mueller Report in 2019 or 2021 Washington Protest)	• To save time and energy while maintaining a very informed and up to date repertoire on security intelligence issues • To anticipate issues before they arise
Threat or Risk Assessments	• Protected documents (for limited distribution) meant to inform on specific events or threats (e.g. COVID-19 Assessment, Building TRA)	• To anticipate issues before they arise • Prevent emergencies • Allow for more informed timely responses when emergencies do occur

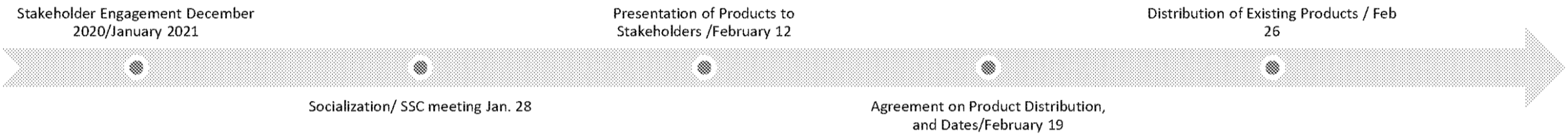
Priority Intelligence Requirements for GE 44

1. Indications and Warnings of a cyber attack on EC's networks.
2. Indications and Warnings of Misinformation/Disinformation with regards to the conduct of an election.
3. Physical security threats to an election, including natural hazards and heath threats.
4. Fraudulent or criminal political activities that could affect the outcome of an election.
5. Deficiencies in internal business processes that could impact the outcome of an election, including business impacted by health threats.
6. Voter accessibility issues which could have an impact on an election, this includes health and safety concerns during a health threat.
7. Electoral perceptions and attitudes towards EC's mandate and services, including perceptions based on any disinformation about the new pandemic procedures.

Annexes – Intelligence Products

Product Distribution

Product	Audience	Total # products (as of date)	Classification	Date available	Distribution method
All Hazards/ ED Studies	Management, Security	175/338 (Jan 13)	Protected B	175 Available upon request, aiming for another 63 by the beginning of March, If the election is delayed we will have them complete in May.	Email on demand for authorized personnel
Single Page ED Summaries	ROs, Field Personnel, Security	338 (Jan 13)	Unclassified//For Official Use Only	175 Available upon request, aiming for another 63 by the beginning of March, If the election is delayed we will have them complete in May.	Email to the ROs for distribution to staff
Security Information / Event Analyses	Management, Security, Interested Stakeholders	28 (Jan 13) Ongoing as reports are published	Unclassified//For Official Use Only	Available upon request	Email on demand for interested stakeholders
Threat/Risk Assessments	Security and specific stakeholder impacted by threat	8	Protected B	Available upon request	Email on demand for authorized personnel



Stakeholder Engagement December 2020/January 2021

Socialization/ SSC meeting Jan. 28

Presentation of Products to Stakeholders /February 12

Agreement on Product Distribution, and Dates/February 19

Distribution of Existing Products / Feb 26

Questions