

Bonvie, Jeff

From: Cameron, Bud
Sent: December-10-12 12:59 PM
To: Dick, Robert
Cc: Hatfield, Adam; Hatch, Roger; Bonvie, Jeff
Subject: FW: Summary of Saskatchewan Tabletop Exercise

Robert, below you will find Roger's summary of the Regina exercise results. I have further summarized into some words you can use for an "fyi" note to Lynda:

As part of our efforts to establish a planning framework for managing cyber incidents outside the government of Canada, two of my staff ran a table top cyber exercise in Regina last week, with a good cross section of players from both provincial/municipal government and critical infrastructure sectors. The Cyber Incident Management Framework (CIMF) document was presented as a draft plan to guide the exercise responses, both to build support for the framework and to solicit immediate feedback for improving it.

The two scenarios were a "pure cyber" event leading to unwanted information disclosure and a "real world consequences" event involving power and water distribution failures. The participants saw great value in the exercise and we observed the usual concerns with sharing cyber incident information – guarding anonymity and preventing public disclosure. The exercise met our objectives of gaining support for the CIMF and the need for timely sharing of cyber incident information, as well as increasing the awareness of CCIRC and its products and services.

Bud

From: Hatch, Roger
Sent: December 9, 2012 10:25 PM
To: Hatfield, Adam; Cameron, Bud
Cc: Bonvie, Jeff; Audeh, Abdul Rahman
Subject: Summary of Saskatchewan Tabletop Exercise

Adam:

As promised, here is a brief summary of the Saskatchewan tabletop exercise held in Regina on Thursday, November 29.

Ultimately, the exercise was a success. We achieved our key objectives, including raising awareness of the Cyber Incident Management Framework (CIMF) across a broad section of provincial, municipal, and CI organizations, while validating the assumptions and expectations contained in the CIMF. We also made a strong case for proactive information sharing, which seemed to resonate with many of the representatives at the exercise.

The objectives of the exercise were:

- Socialize the current version (v0.9) of the CIMF with a broad cross-section of provincial and municipal representatives, as well as members of critical infrastructure owners and operators from many sectors, and solicit feedback towards the completion of the first working draft (v1.0).
- Conduct a pair of tabletop exercises to validate or expose errors in assumptions and expectations currently contained within the CIMF, and to gain a better understanding of the culture and processes inside provincial, municipal, and CI organizations with respect to incident reporting and information sharing.

- Advocate for the proactive sharing of information within the cyber security community within Canada to heighten the effectiveness of cyber preparedness and response, and increase awareness of the services and products provided by CCIRC.

A significant cross-section of the cyber security community was represented at the exercise, including:

- Public Safety Canada, both from Ottawa (Ken Bendelier and myself) and from the Regional Office (James Gulak)

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

The two scenarios we employed for the exercise were:

- Scenario 1: A “traditional” cyber security threat, including the successful infiltration of multiple organizations via a keylogger malware, leading to information disclosure.
- Scenario 2: A “real world” consequence management event, involving the failure of power generation and water distribution, that is later determined to have been caused by an exploit of control system vulnerabilities.

Scenario 1 played out largely as expected. Some organizations were quick to move to information sharing, as long as it could be done in an anonymous fashion, while others expressed a desire to conduct a thorough analysis and determine many of the details on the attack before sharing information. A common concern was the public disclosure of information, including through ATIP, which showed as a significant impediment to full information sharing. A significant discussion also ensued regarding the need for organizations to establish their own incident severity matrix, with thresholds for escalation and reporting that make sense for their organization’s size, business sector, and other factors; the Government of Canada model (prepared by CCIRC) has been provided for reference purposes through the CIMF, but the thresholds within that model are not scaled for provincial governments or private enterprises.

A number of CI operators, particularly in energy and manufacturing, highlighted their continuing ability to operate without information systems for an extended period without significant impact to their core business; of course, the opposite was true for others, including [REDACTED]

As the scenario unfolded, a general awareness grew amongst the scenario players and observers that more proactive sharing of incident information is required and will help strengthen community responses to cyber incidents; in side conversations, several CI operators referenced their appreciation for the cyber flashes they receive from CCIRC, and acknowledged that it was time they began contributing to the community knowledge base and become a provider of information as well as a consumer.

Scenario 2 was effective in highlighting some of the coordination, communications and public affairs challenges associated with events that cross the boundary between cyber and emergency management. The scenario itself can be strengthened for future exercises by ensuring the scenario events force an engagement with certain government agencies, such as the GOC, and by detailing an extended timeframe that separates some of the early consequence management and system restoral (using manual overrides, if required) from the later fault isolation and cyber-related investigation.

In all, the participants expressed appreciation for the day’s activities and stressed that they saw great value in participation in these types of activities. While we did not receive specific feedback on the CIMF document itself, that was not the intent of the day’s activities; we did gain a lot of insight that should help with fleshing out the CIMF, and I expect to receive some feedback as the attendees review the CIMF in the context of the exercise scenarios.

Please let me know if you require any additional details at this time.

Thanks,

Roger Hatch, PMP CISSP CISM ABCP

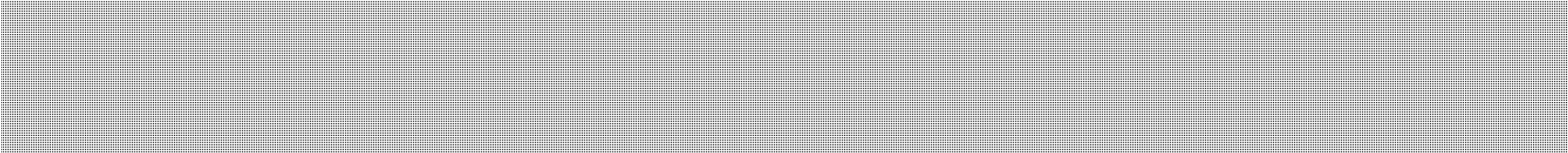
Senior Analyst

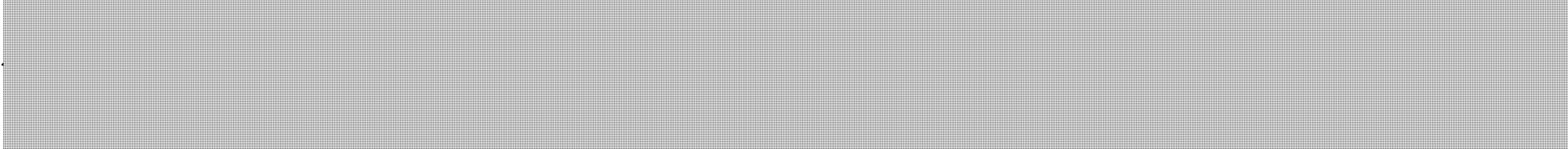
roger.hatch@ps-sp.gc.ca

(613) 993-5026

s.16(2)(c)

Exercise Summer Heat

- The purpose of this exercise was to identify gaps in the current response mechanism to a cyber incident external to the federal government.
- 
- Participants from PS (CCIRC, GOC, PS Comms, NS Ops), CSEC, CSIS, RCMP, DND/CF attended
- For actions taken by partner departments, please see the meeting notes (RDIMS 672246).



Issues/Questions

- The concern was not so much for the cyber incident, rather any resulting effects (i.e. a power outage, especially if the US was affected). This is what dictates any federal government course of action.
- Not clear on how to determine if/when the power goes out. Only the power plant can answer that.
- Not clear what the federal government could actually do. The federal government does not “solve” the problem for the affected entity, only coordination and providing advice. Ultimately it’s up to the entity to fix the problem.
- The effected entity must ask for assistance. Even then, they are not required to accept federal government help and the federal government cannot impose or force the entity to do anything.
- Escalation depends on the effects (economic, health and safety, etc.) of the cyber incident.
- Challenges Arose regarding the roles and responsibilities of partners involved in the federal response (this is what the CIMF and FCCP are intended to address).



Public Safety
Canada

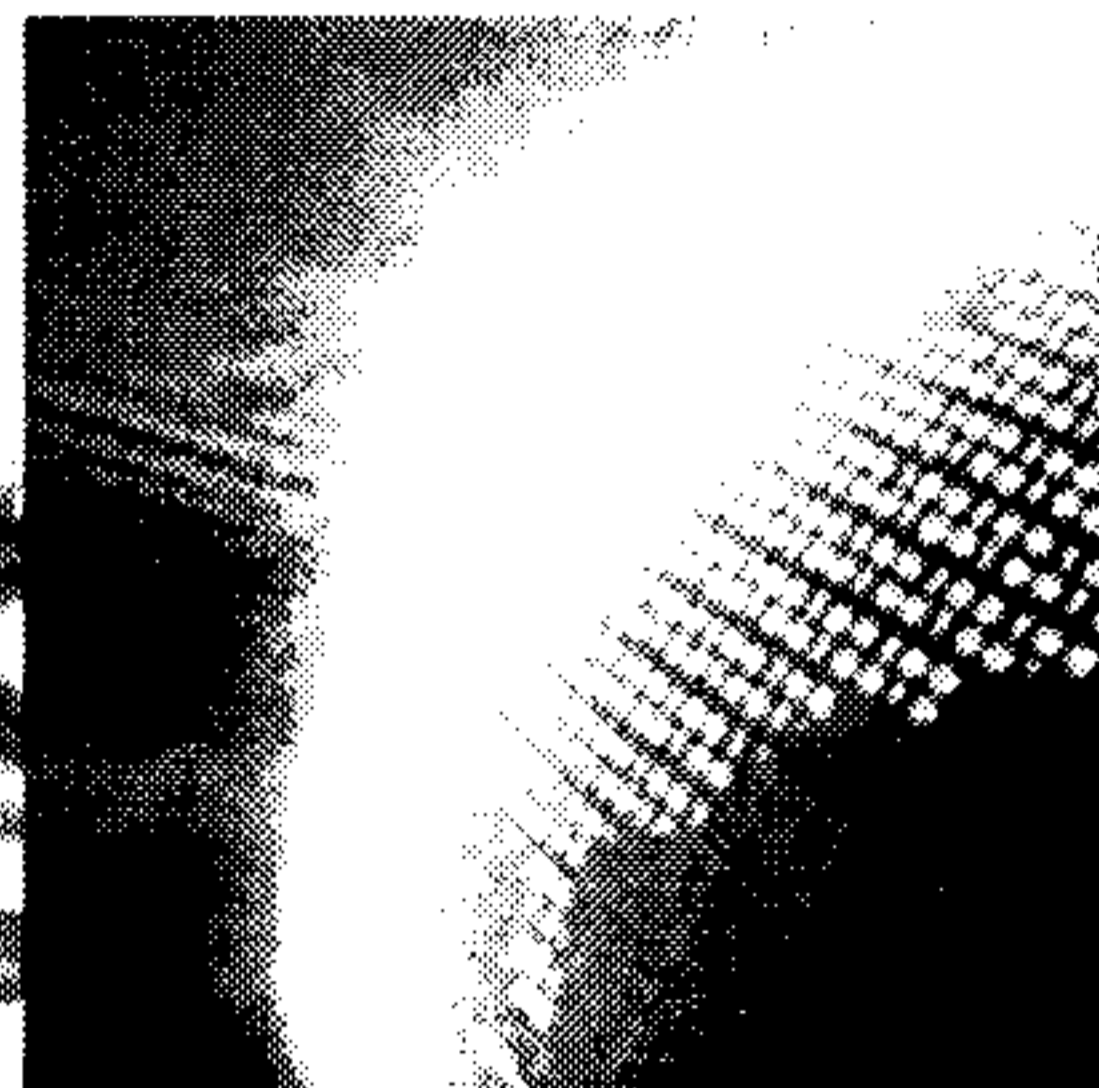
Sécurité publique
Canada

BUILDING A SAFE AND RESILIENT CANADA



Exercise SPRING THAW

After Action Report



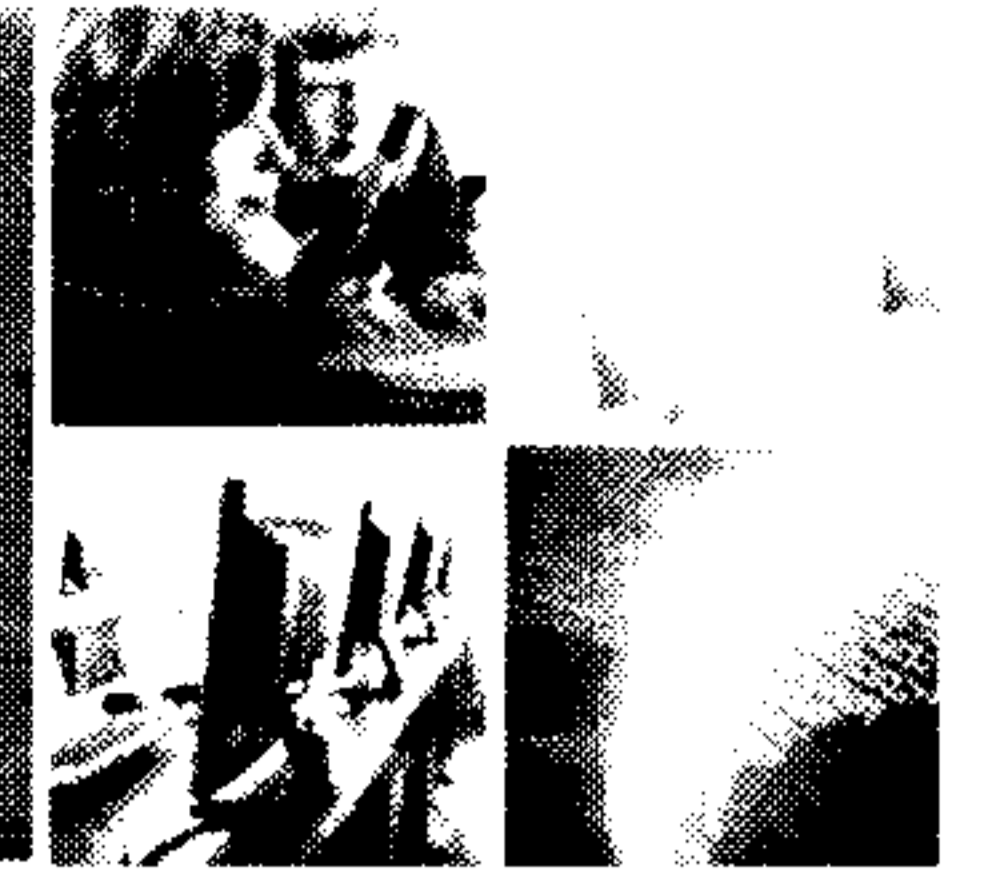
RDIMS #620198

Canada

000005

FOR EXERCISE EYES ONLY

Exercise Attendees



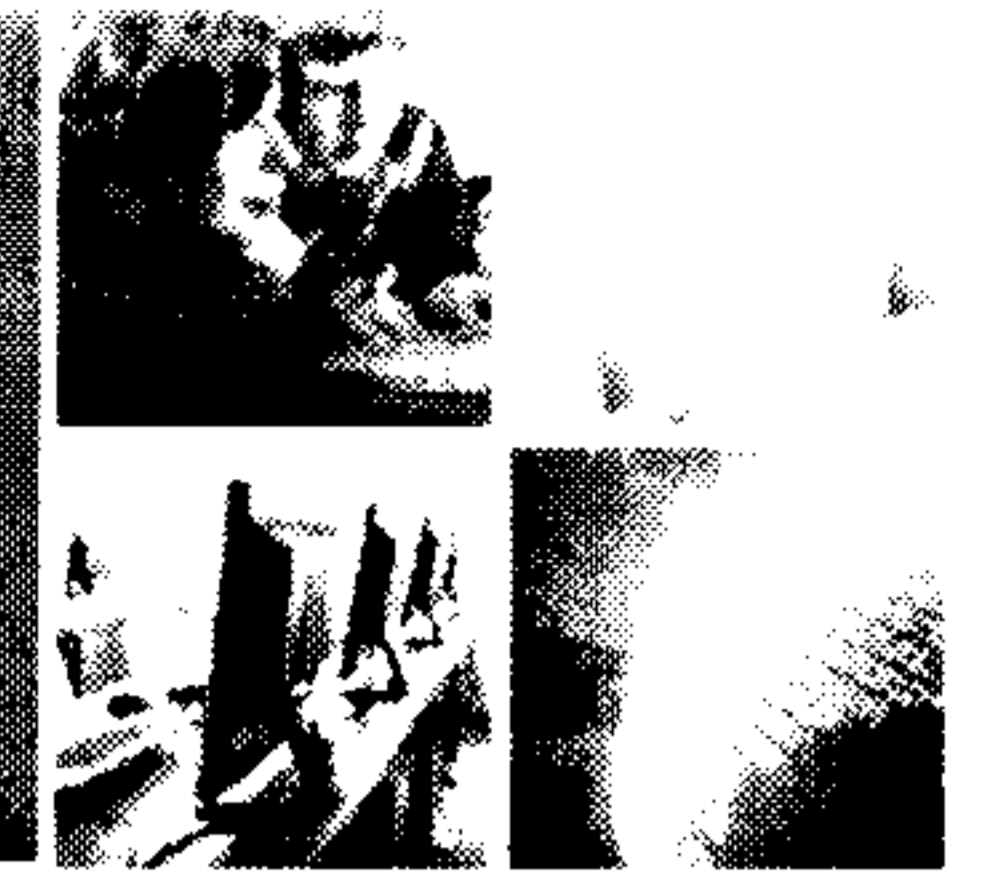
BUILDING A SAFE AND RESILIENT CANADA

- Players
 - PS
 - CSEC
 - RCMP
 - CSIS
- Observers
 - DRDC
 - PS
 - NCSD staff, Legal, Comms



FOR EXERCISE EYES ONLY

Exercise Overview – Scenario #1



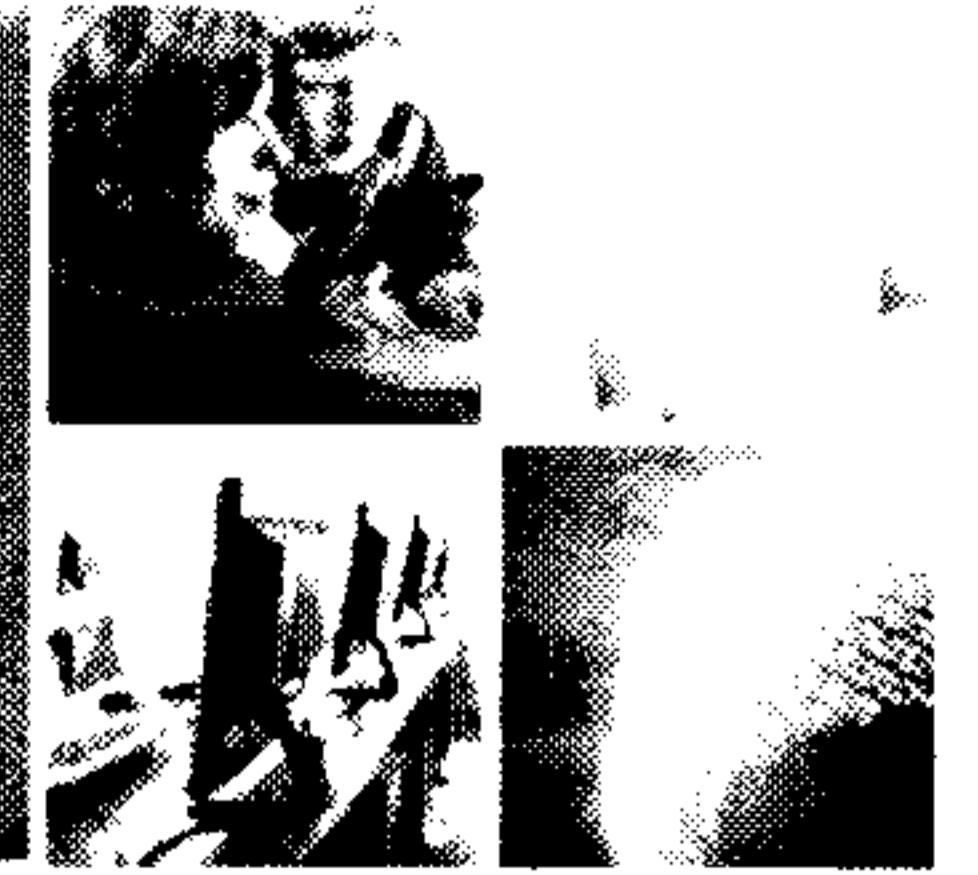
BUILDING A SAFE AND RESILIENT CANADA

- Request by provincial government to Royal Canadian Mounted Police (RCMP) for assistance
- Increased media attention
- Problems reported at Black Horse Falls and the potential for increased power disruption and non-cyber related events (consequence management)
- Request by Newfoundland Power for Canadian Cyber Incident Response Centre (CCIRC) assistance
- Government Operations Centre (GOC) has been in contact with:
 - Natural Resources Canada
 - CCIRC
- Natural Resources Canada Communications Branch has contacted the GOC for information
- Department of Homeland Security has contacted the GOC over concerns of power disruptions



FOR EXERCISE EYES ONLY

Exercise Overview Scenario #2



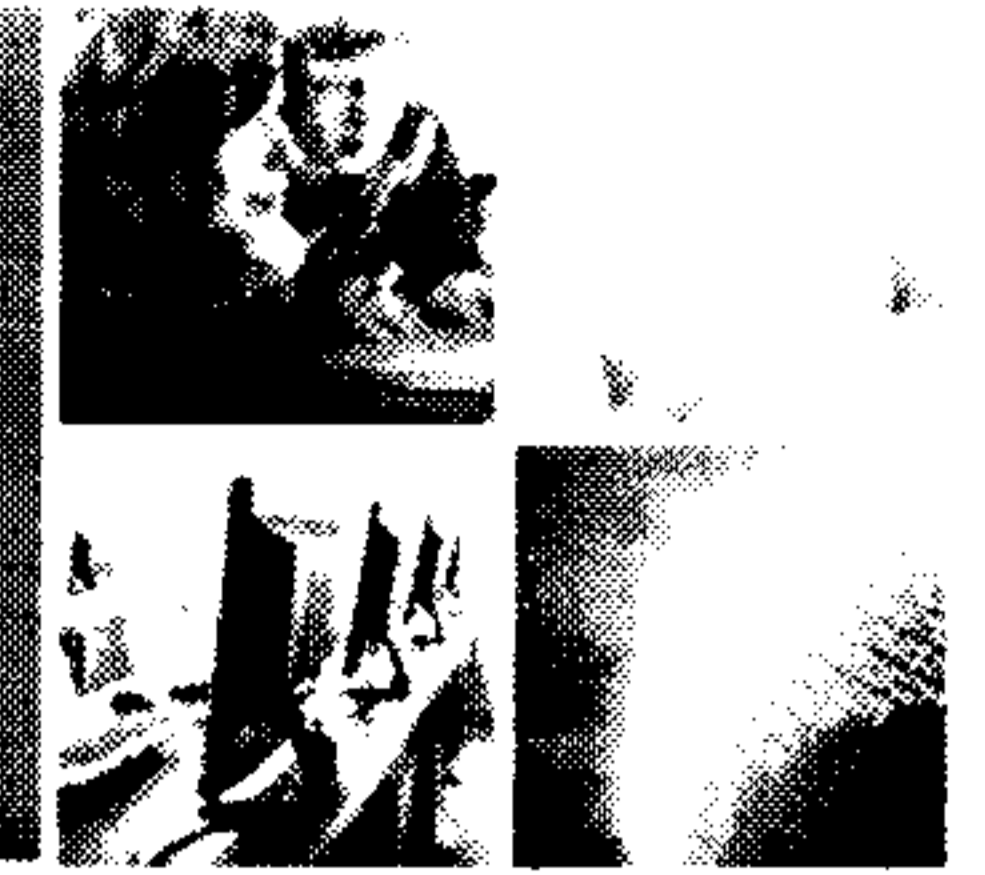
BUILDING A SAFE AND RESILIENT CANADA

- Compromise of provincial government network
- RCMP investigation with cross border implications
- Potential manipulation of a strategic procurement initiative
- IP addresses
 - Of interest to Canadian Security Intelligence Service (CSIS)
 - Known to Communications Security Establishment Canada (CSEC)
- Potential for widespread infections in Canada
- Impact to Canada and Canadians
- Private cyber security firm announcement
- Attribution to known state sponsored actors



FOR EXERCISE EYES ONLY

Observations (1/?)



BUILDING A SAFE AND RESILIENT CANADA

No easy escalation mechanism:

- Escalation determined by perceived impact – [REDACTED] and no unified brief available
- Inconsistencies on when departments would brief their management – depends on ...
- Briefing up would occur prior to briefing laterally



FOR EXERCISE EYES ONLY

Observations (1/2)



BUILDING A SAFE AND RESILIENT CANADA

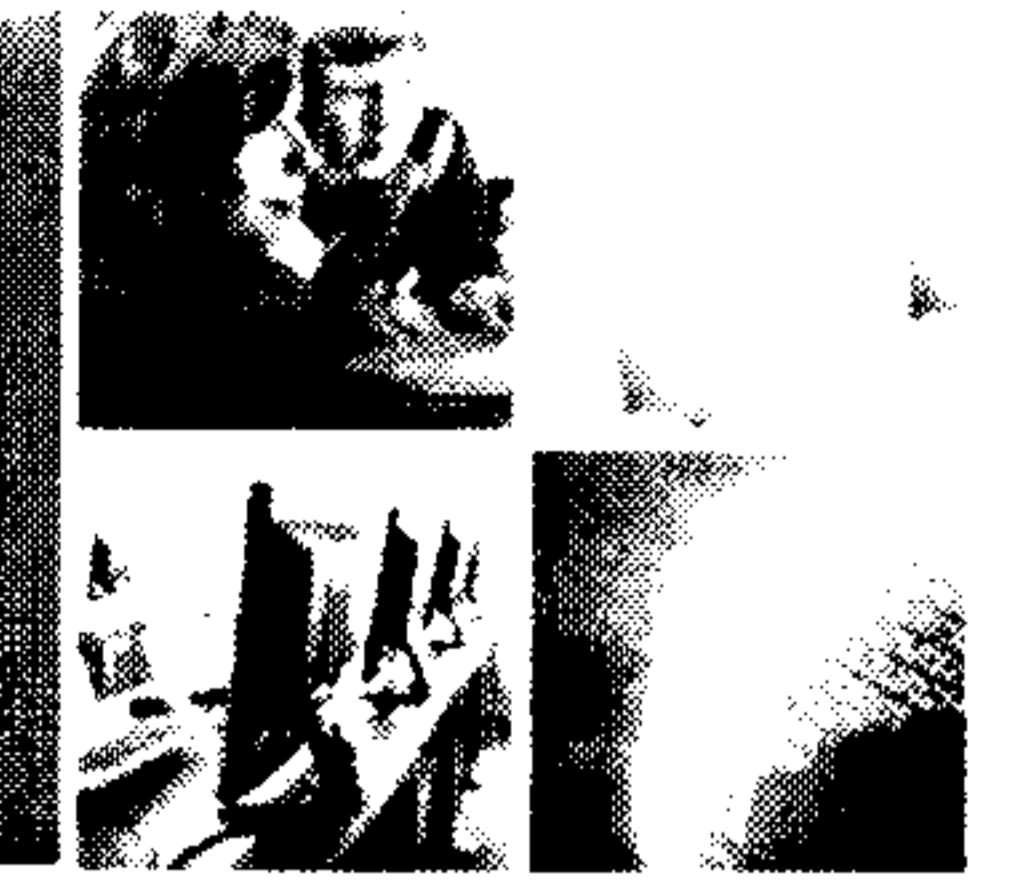
[Redacted]

- [Redacted]
- [Redacted]
 - Meeting of concerned parties is based on existing/former relationships
- [Redacted]

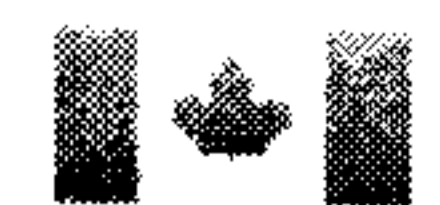
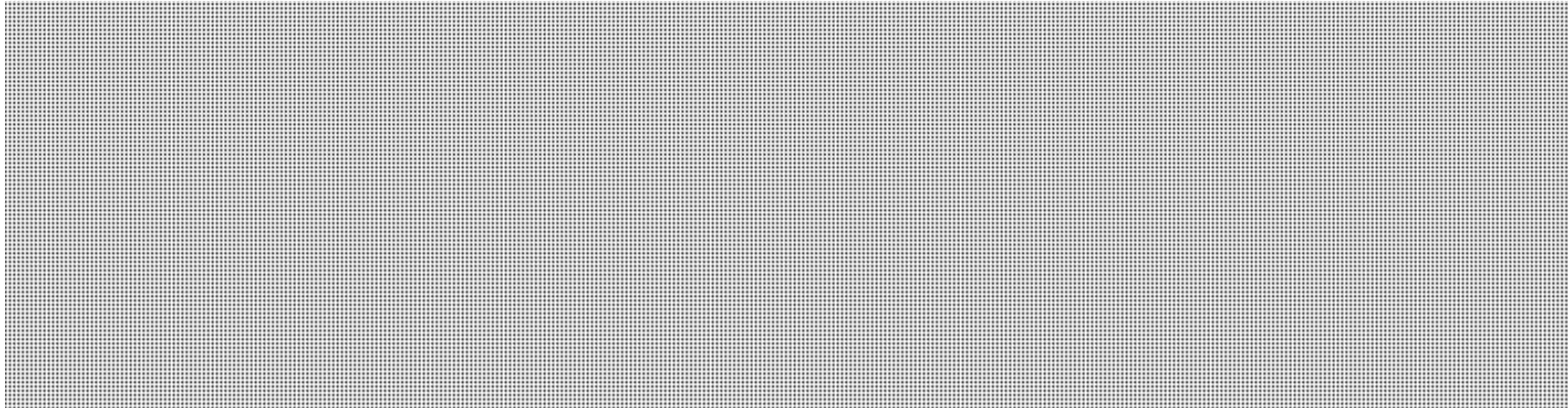


FOR EXERCISE EYES ONLY

Observations (2/2)

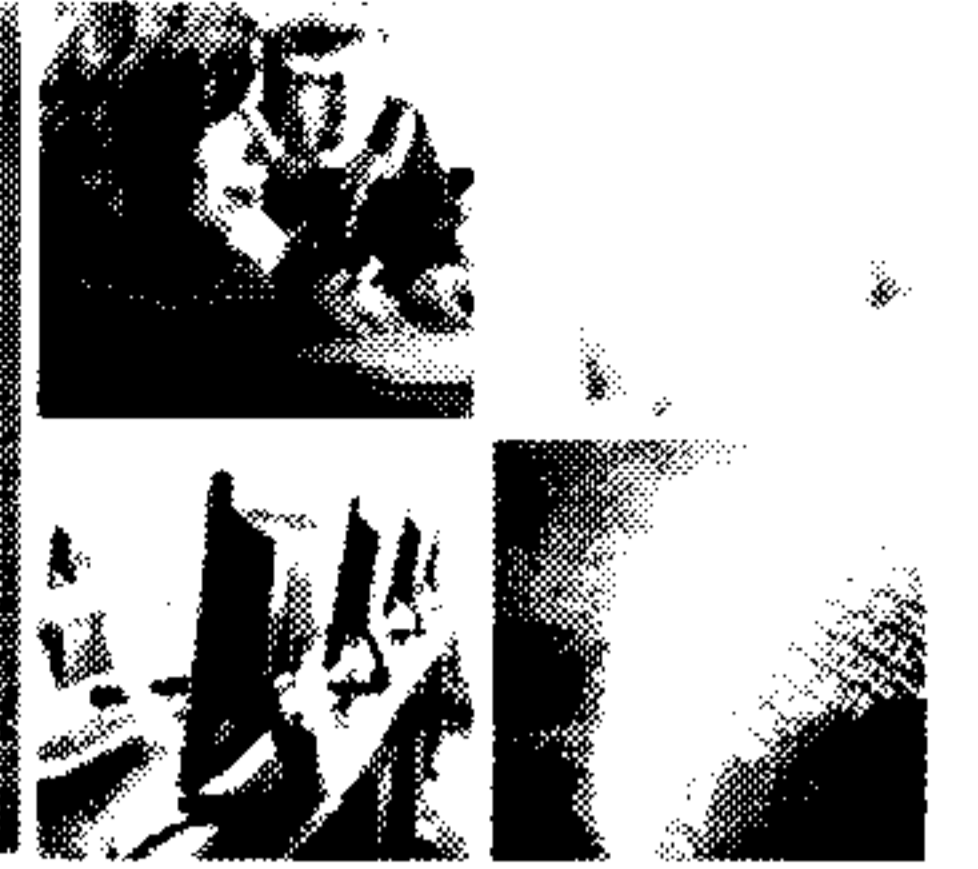


BUILDING A SAFE AND RESILIENT CANADA



FOR EXERCISE EYES ONLY

Next Steps



BUILDING A SAFE AND RESILIENT CANADA

- Memo to Public Safety ADM NS
- Engage within Public Safety
 - Government Operations staff
 - National Security staff responsible for ADM NS
 - Potential linkages between DG Cyber Ops and ADM NS
 - Critical Infrastructure
- Conduct table-top exercise at Director level
 - Event to be escalated to ADM NS and GOC
 - Include sector lead departments (NRCan and Finance)
 - Select private industry (Energy sector and financial institution)

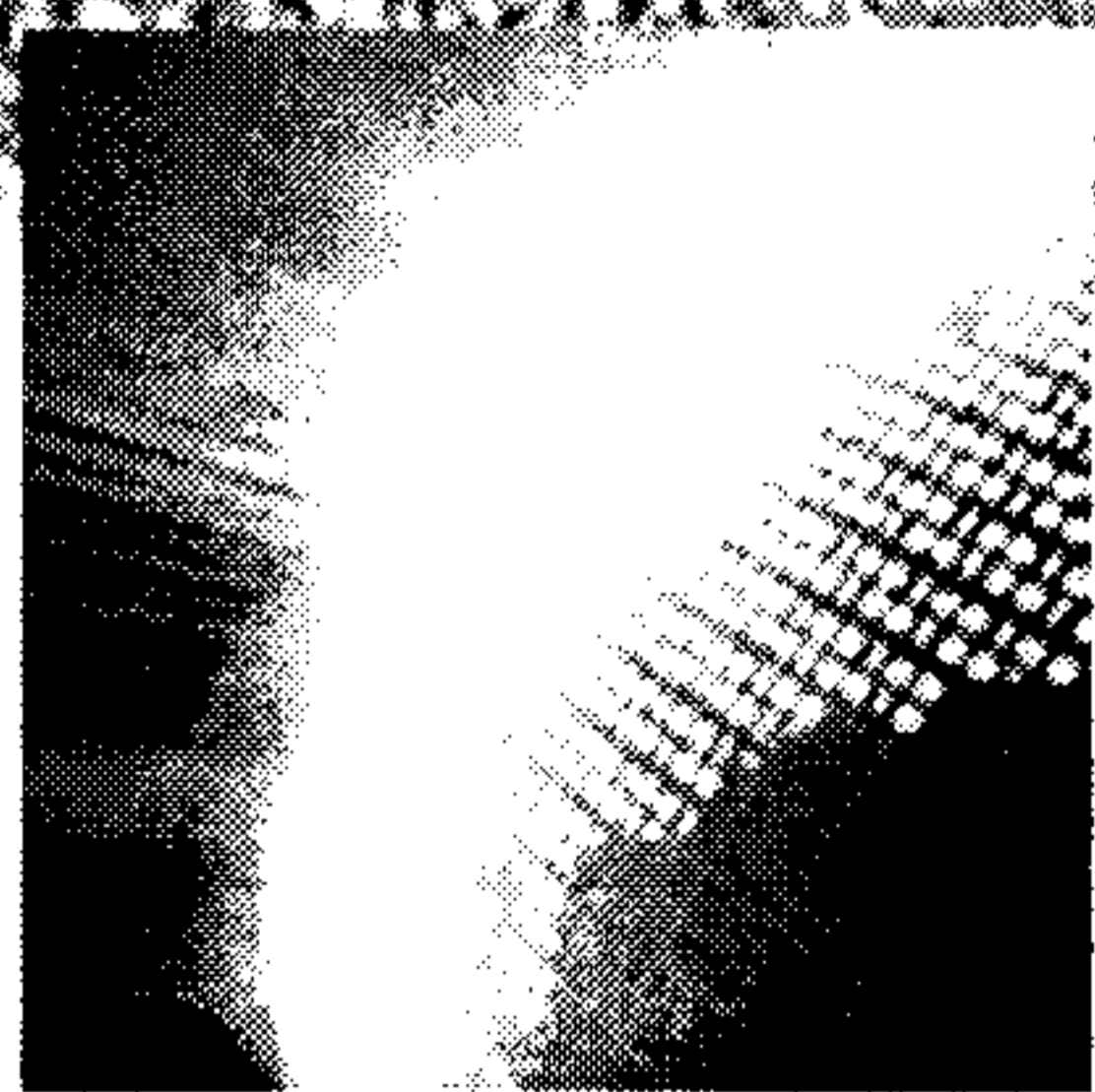
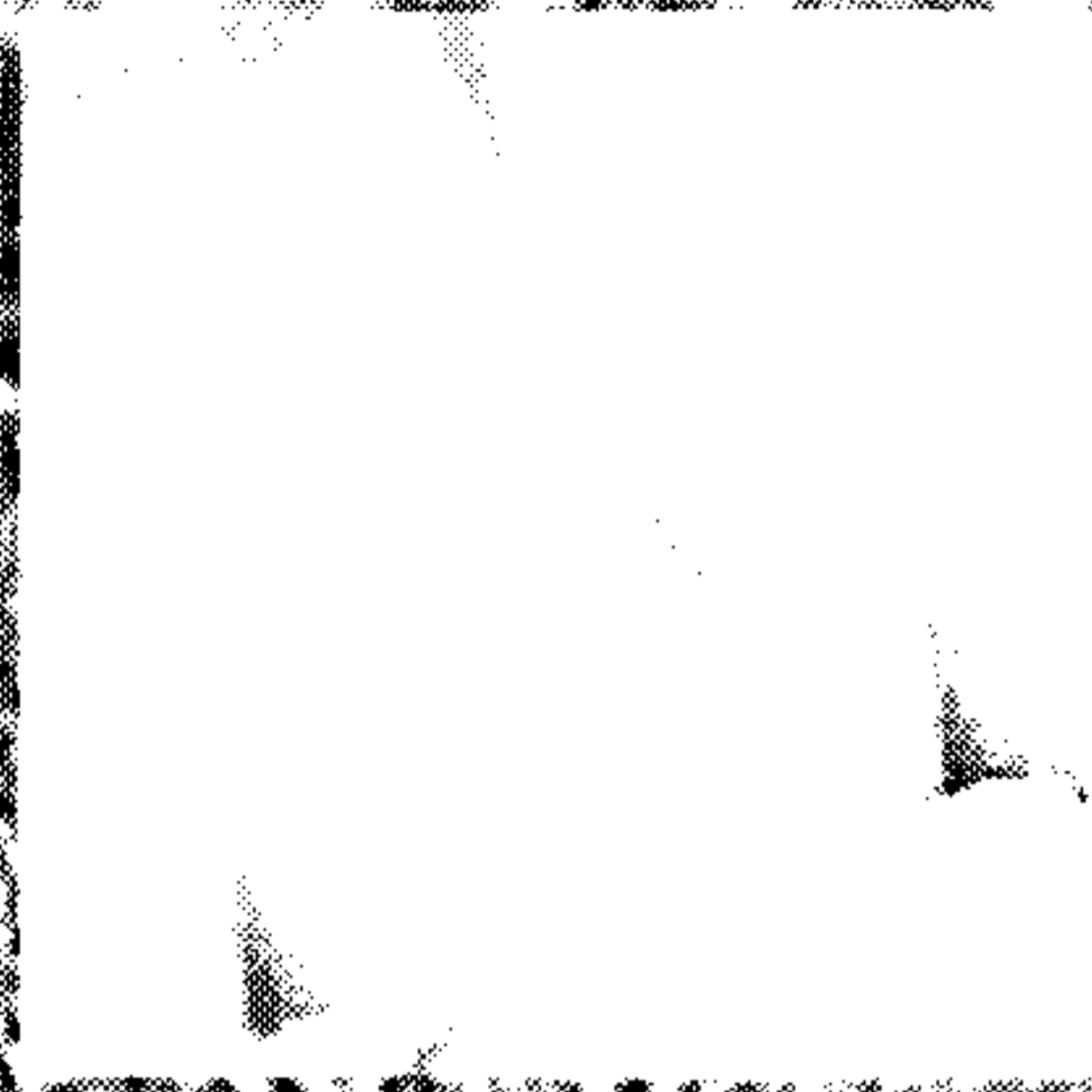




Public Safety
Canada

Sécurité publique
Canada

BUILDING A SAFE AND RESILIENT CANADA



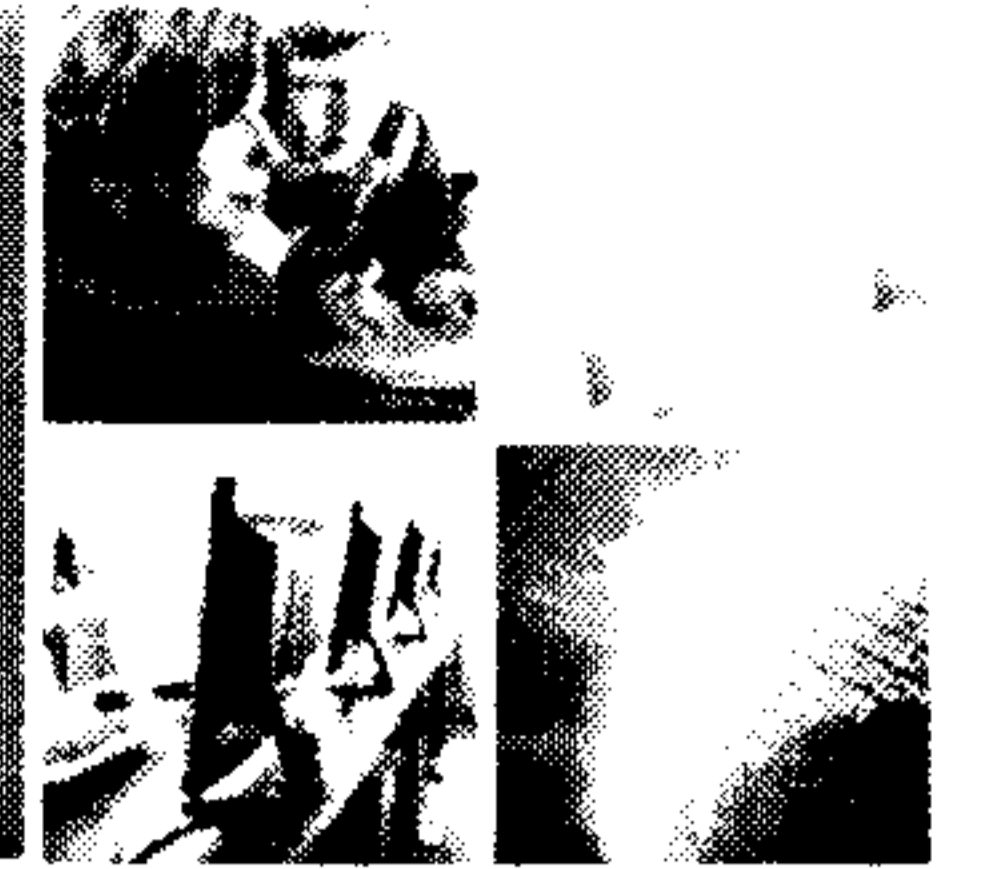
Exercise FROZEN POND After Action Report



Canada

FOR EXERCISE EYES ONLY

Exercise Attendees



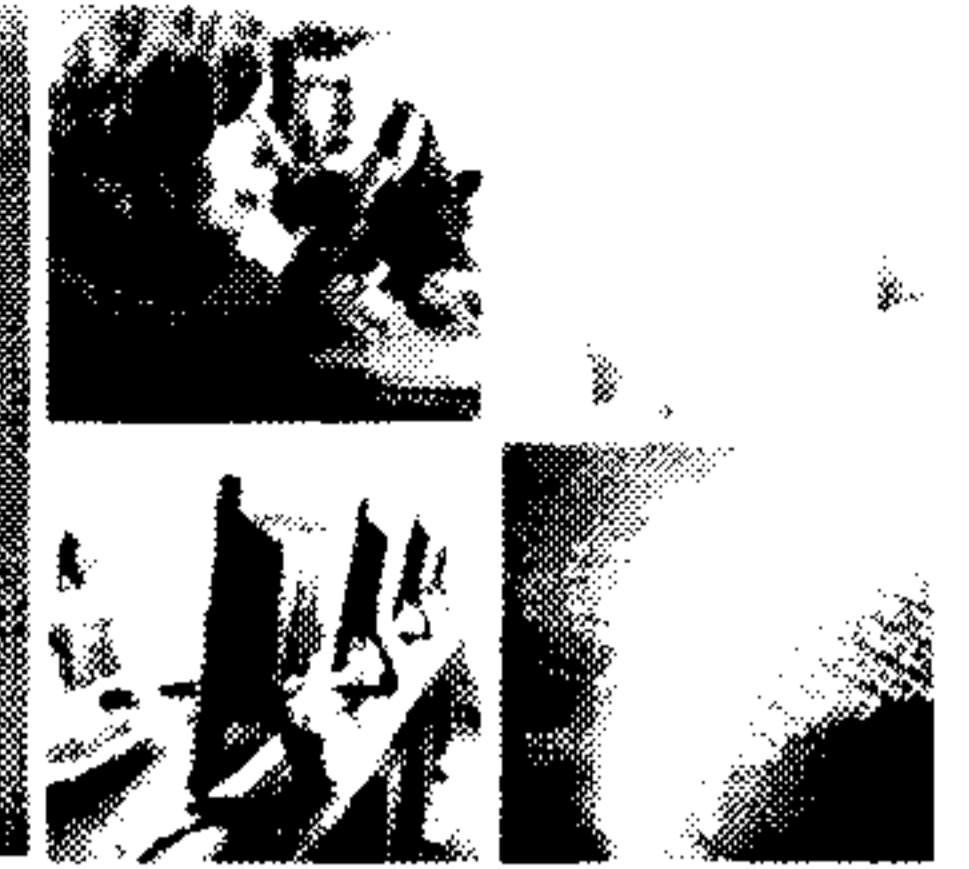
FOR A SAFE AND RESILIENT CANADA

- Players
 - PS/CCIRC
 - CSEC/CTEC
 - RCMP/Tech Crime
 - CSIS/████████
 - CF/CFNOC and DND/CDI
- Observers
 - PS/NCSD, CI, Legal, Comms, Ex, GOC
 - DND/DRDC, ADM Pol, Canada COM
 - IC
 - TBS/CIOB
 - CSEC/Pol



FOR EXERCISE EYES ONLY

Exercise Overview (1/3)



FOR A SAFE AND RESILIENT CANADA

- B1nary Brotherhood (offshoot of Synonymous), hacktivist organization unhappy with Canada's exploitation of natural resources
- CSIS and CCIRC aware of the group
- CCIRC receives reports from Province of Alberta and OilCo of spoofed e-mails
 - Sends files to CSIS and CSEC for analysis
- Analysis
 - Zero day exploit
 - Keylogger with new file and links to Montreal based ISP

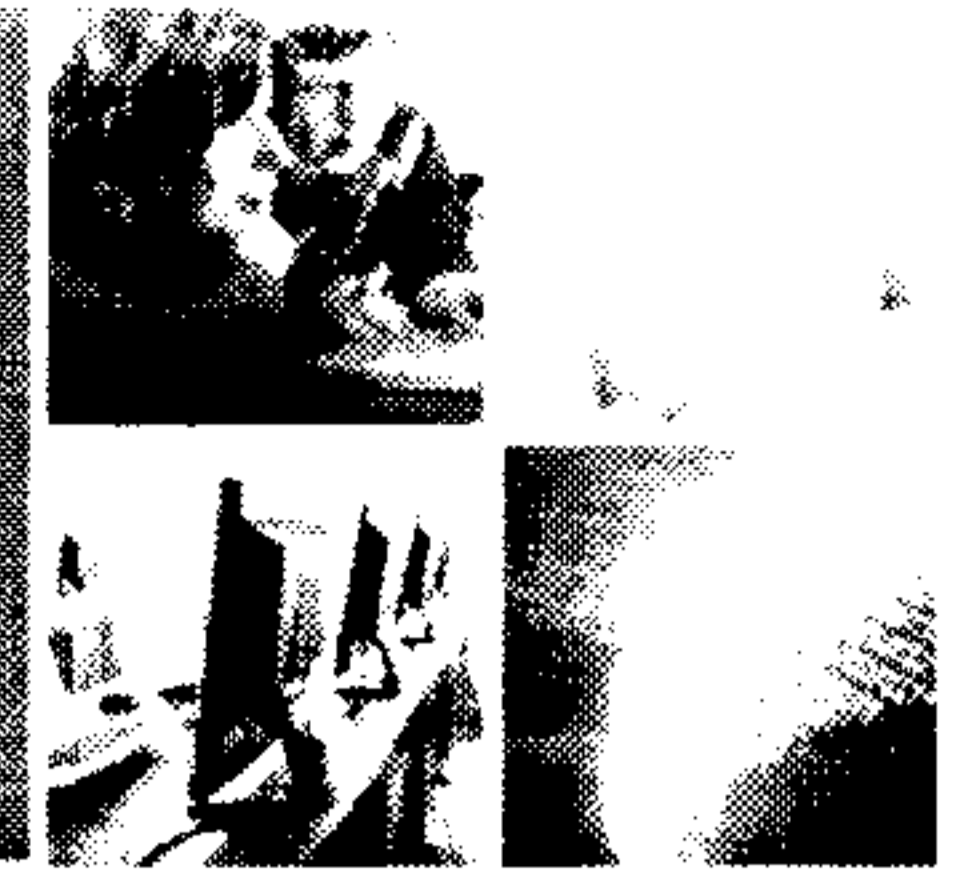


Public Safety
Canada

Sécurité publique
Canada

FOR EXERCISE EYES ONLY

Exercise Overview (2/3)



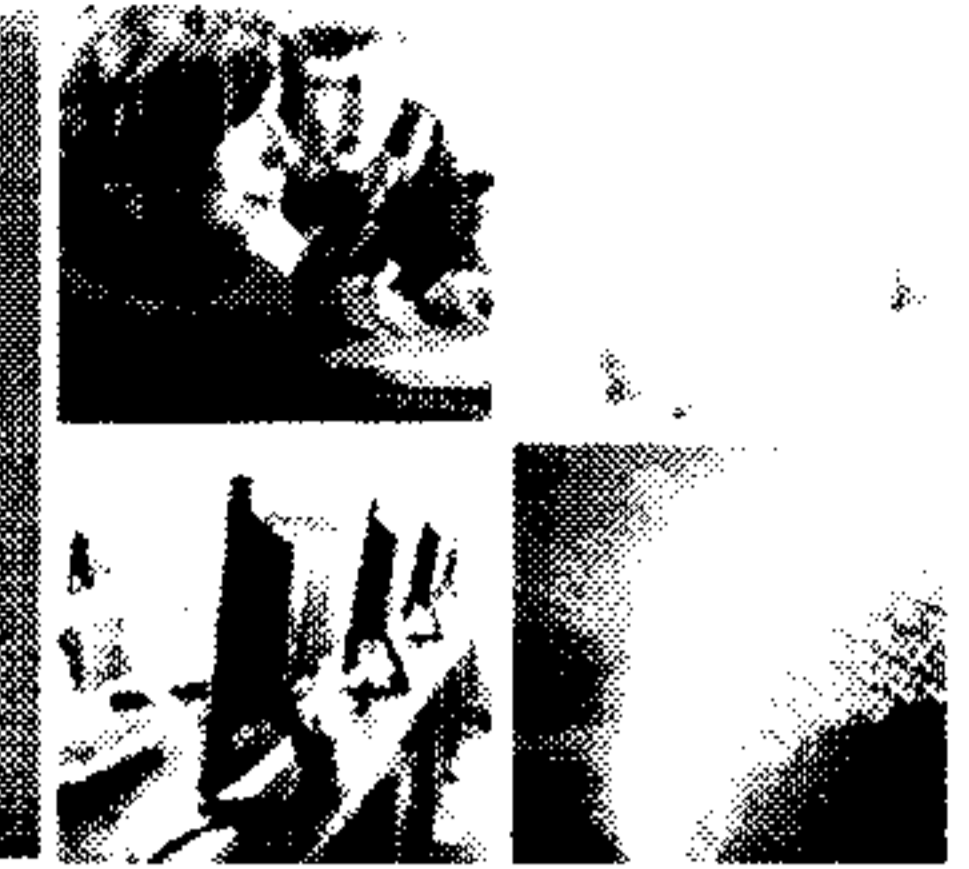
FOR A SAFE AND RESILIENT CANADA

- CSEC links to known GC attacks
- Related to DND/CF investigation
- CCIRC receives UK media reporting on planned B1nary Brotherhood attacks
 - UK requests intelligence
 - GOC receives media requests
- Oilco asks for CCIRC mitigation assistance
- CCIRC asks for RCMP assistance to take down web site in Montreal
 - No legal mandate for RCMP to do this
- CCIRC receives additional reporting of spoofed e-mails from energy companies



FOR EXERCISE EYES ONLY

Exercise Overview (3/3)



BUILDING A SAFE AND RESILIENT CANADA

- Web hosting company complies and provides additional targets (AB government, oil sands companies and TSX)
- CCIRC contacts TSX
 - TSX advises infections and requests assistance
- CCIRC analysis of new file related to foreign IP
 - Linked to CSIS and CSEC investigations
 - Payload timed to format hard drive
- Multiple requests from energy companies and AB Gov for assistance from CCIRC

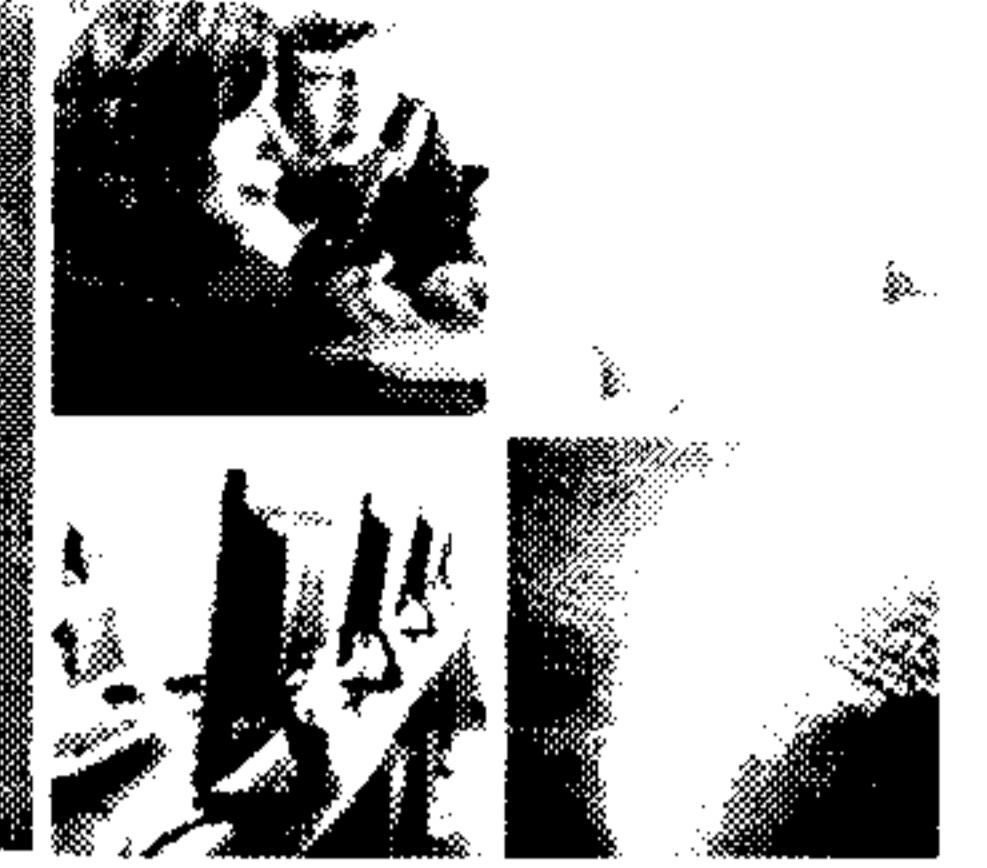


Public Safety
Canada

Sécurité publique
Canada

FOR EXERCISE EYES ONLY

Observations (1/4)



BUILDING A SAFE AND RESILIENT CANADA

[Redacted]

- [Redacted]
- [Redacted]

- Meeting of concerned parties is based on existing/former relationships

- [Redacted]

- Not clear if / how CCIRC can exploit partners' mandates
 - E.g., not DND/CF's mandate to support CCIRC for non-federal government network incidents

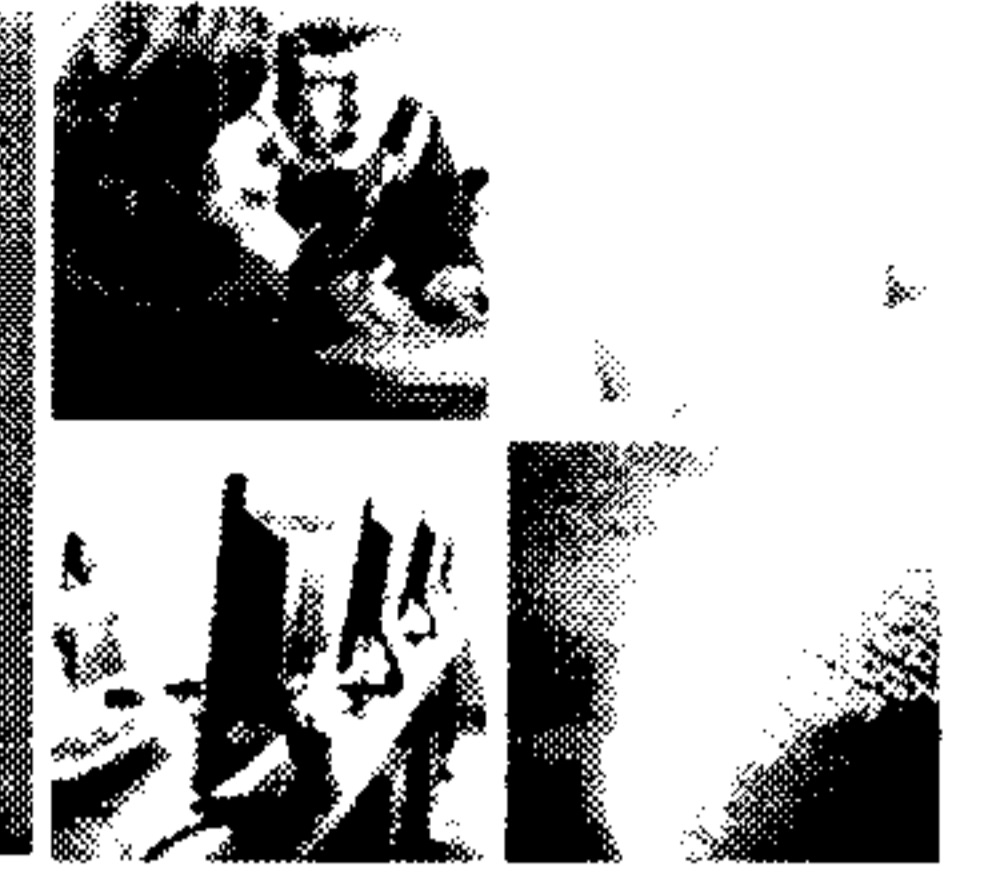
- RCMP, CSEC and CSIS technical analysis [Redacted]

- [Redacted]

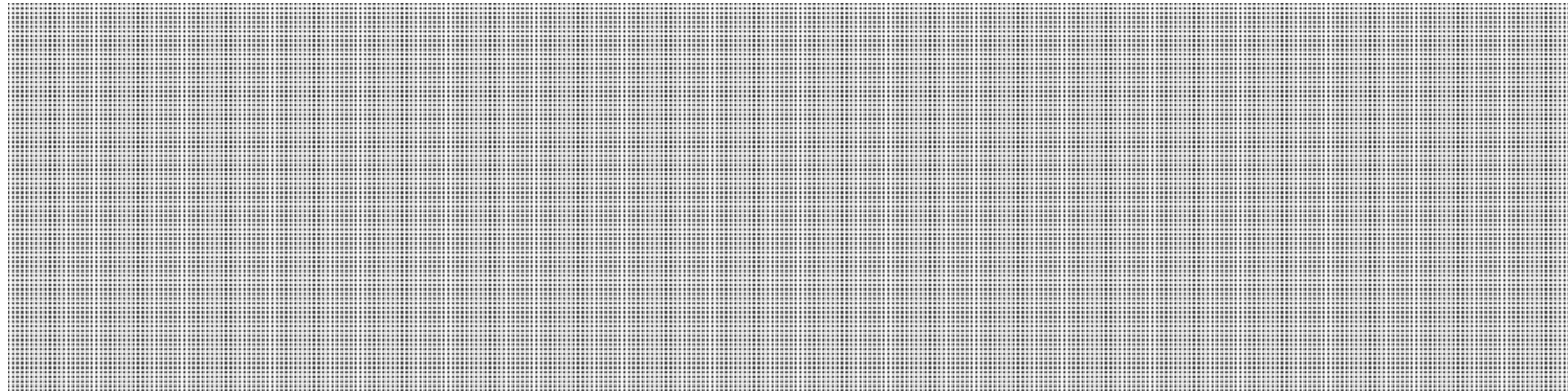


FOR EXERCISE EYES ONLY

Observations (2/4)



BUILDING A SAFE AND RESILIENT CANADA



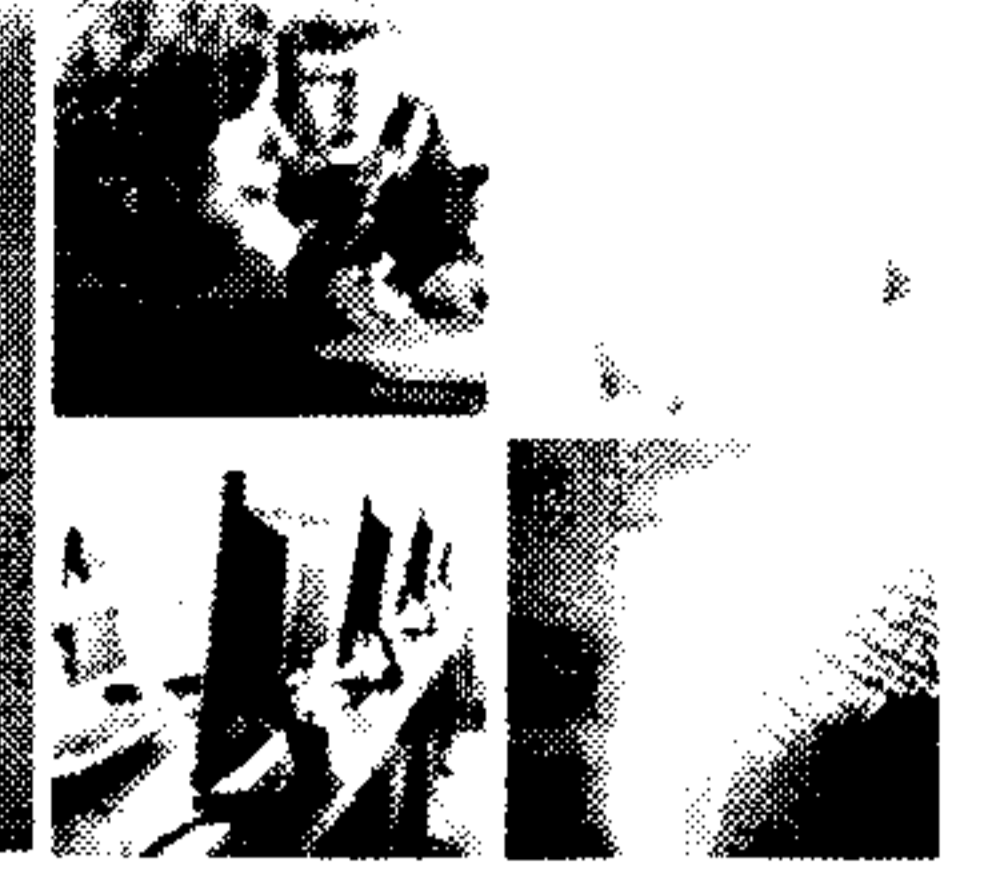
- Recognition that CCIRC should be lead (amongst cyber agencies) in dealing with affected entity

- [Redacted]



FOR EXERCISE EYES ONLY

Observations (3/4)



ENFTE 115 - SAFE AND RESILIENT CANADA

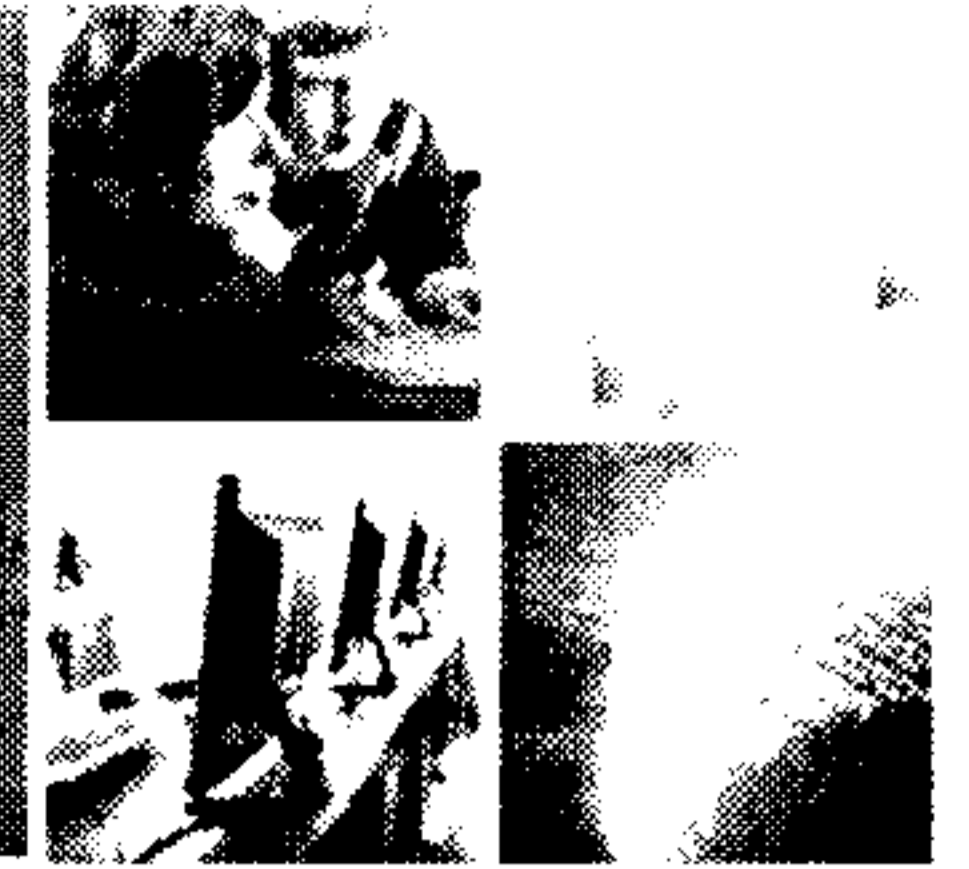
No easy escalation mechanism:

- Escalation determined by perceived impact – as stated, [REDACTED] and no unified brief available
- Inconsistencies on when departments would brief their management – level of interest
 - [REDACTED]
- Current escalation route is to GOC, which:
 - [REDACTED]
 - [REDACTED]
 - Exercised during CyberStorm III



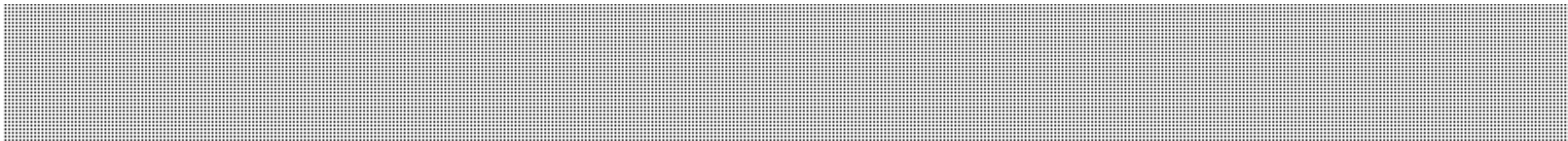
FOR EXERCISE EYES ONLY

Observations (4/4)



BUILDING A SAFE AND RESILIENT CANADA

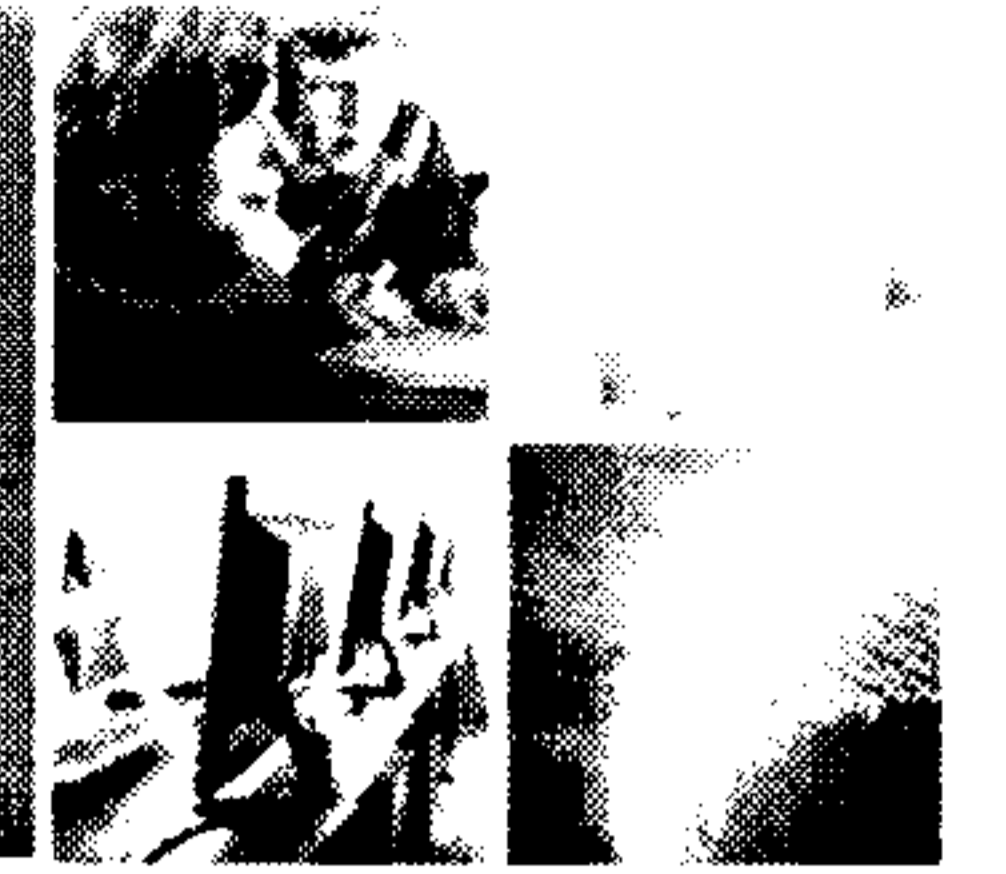
Government role unclear:

- 
- Should the GC provide mitigation or defensive assistance to a non-federal entity?
 - Duty of care?
 - RCMP would assist (provincial responsibilities)
 - What if Premier called asking for assistance?
- Unlike in EM, Government is NOT a force of last resort in cyber (mitigation or defensive role)
- Requirement for effective communications plan
 - Across GC departments
 - With affected PT, CI or entity



FOR EXERCISE EYES ONLY

What Worked Well, But...



BUILDING A SAFE AND RESILIENT CANADA

- Based on current relationships, key partners (old CTU) met
- Roles were well understood

But

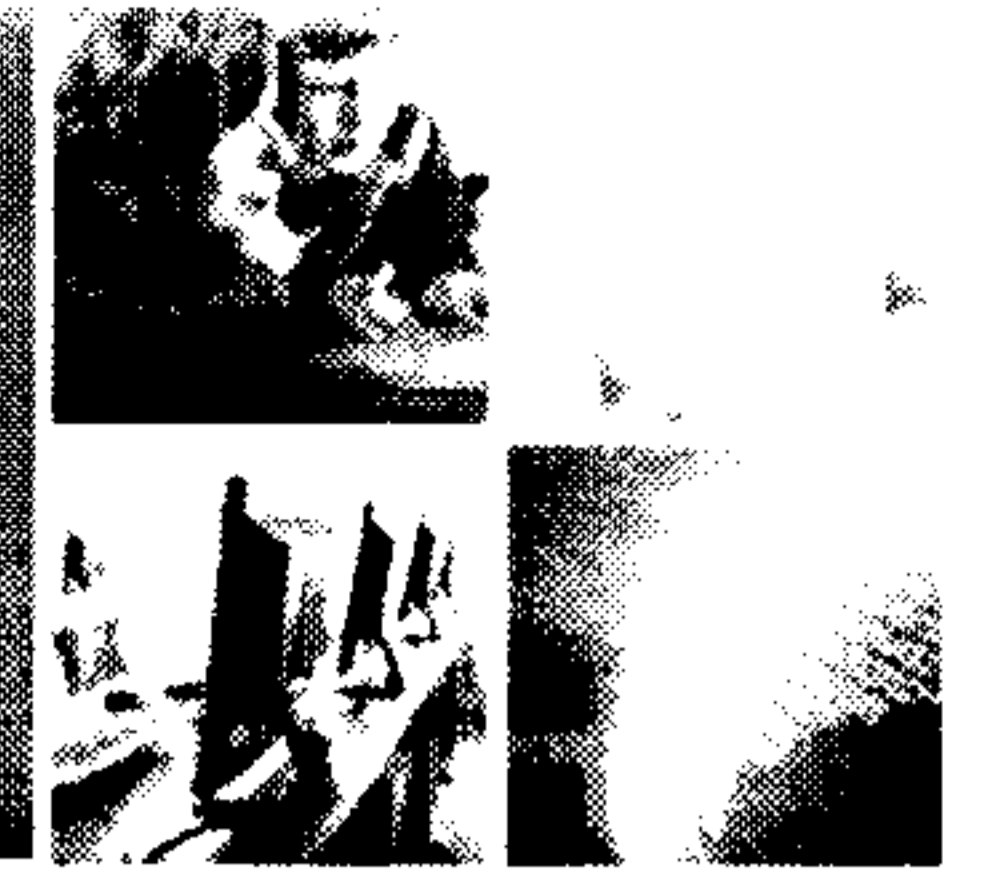
- CSEC needs written permission to share CCIRC provided information with CTU partners
- Require unified brief to senior decision makers
- Policy issues
 - Response to “state sponsored”
 - Premier request

- [Redacted]



FOR EXERCISE EYES ONLY

Next Steps



BUILDING A SAFE AND RESILIENT CANADA

- Brief DG Cyber
 - 10 minute debrief? 30 minute run-through? Tabletop exercise?
- Engage Emergency Management staff
- CCIRC to improve SA
- National cyber incident response framework
 - Engage partners (Fed, PT, CI and select others)
 - Build on existing CCIRC relationships
- Conduct additional exercises
 - Include sector lead departments
 - Provinces / territories
 - CI sectors
 - Select private industry

