TS/ /CEO

SITE Task Force

Progress Update to ADMs

30 August 2019

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

AGENDA

CSE CSIS

GAC RCMP

1. Threat Updates

2. Operational Readiness

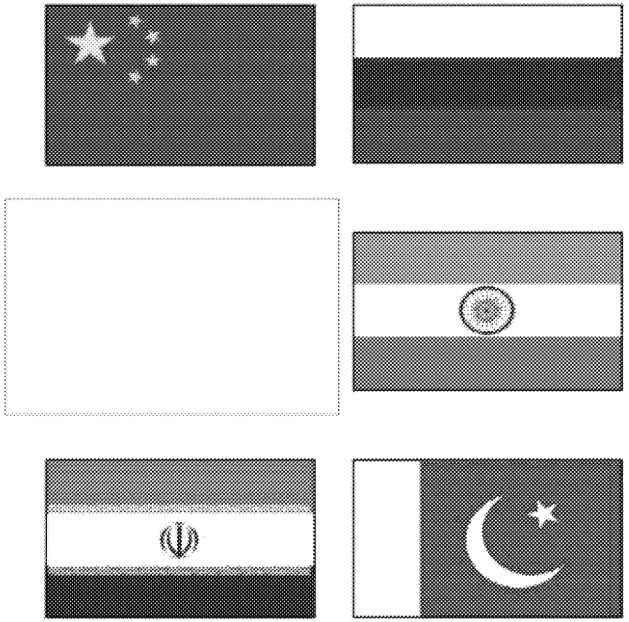
i. SITE TF Response Matrix

ii. SITE TF SITREP

iii. SITE TF Surge Postures

3. Engagements

Threat Updates



China

- SITE continues to observe China engaging in interference activity domestically, seeking to influence and interfere with Canadian persons and organizations supportive of the "five poisons".

Russia

- [redacted]
- [redacted] not observed Russia directly targeting Canada's electoral security or democratic processes. [redacted]

[redacted]

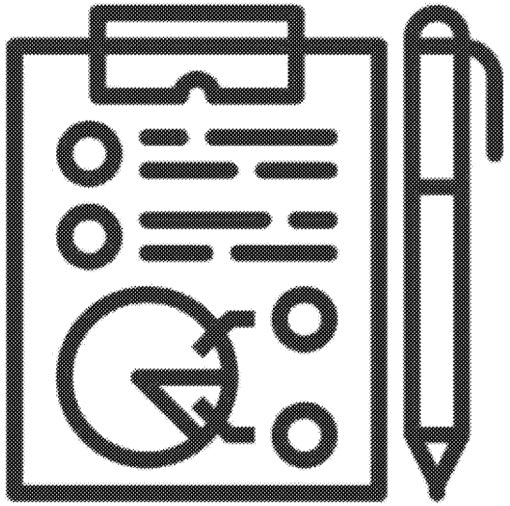
India

- [redacted]

Iran and Pakistan

[redacted]

SITE TF Response Matrix



Creating a Response Options Menu

- SITE's Response Matrix is based upon SITE's 5 identified categories of foreign interference.
- The Matrix provides a high-level overview of the different response options SITE could take in response to foreign interference, as well as the associated levels of risk.
- Within the Matrix, risk is defined as reputational risk to the Government of Canada which includes, amongst other things, the perception of bias, ineffectiveness and overstepping the respective authorities of SITE TF agencies.

S/[redacted]/CEO

SITE Response Matrix

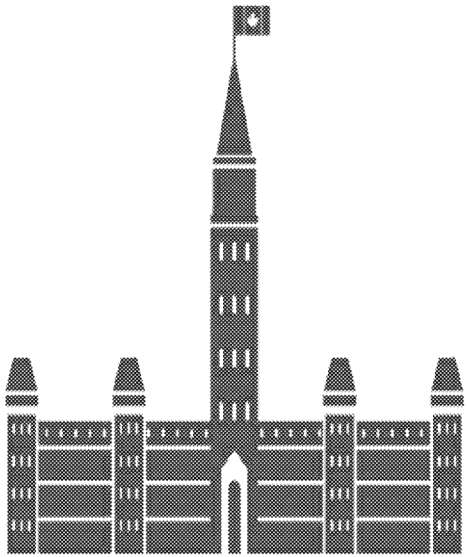
1	2	3	4	5
Cybersecurity Threats against Electoral Infrastructure	**Cybersecurity Threats against Political Parties & Government Officials**	**Covert Political Interference**	**Covert Public Interference**	**Overt Influence**
MONITOR LOW **CSE** (CCCS)/**CSIS:** investigate attack and establish indicators **CSE (SIGINT)/GAC:** support with additional intelligence		**MONITOR** LOW **CSIS**: collect additional intelligence, [redacted] (TRM) **CSE** (SIGINT): collect additional intelligence via regular collection or covert online ops against foreign account **GAC**: outreach to trusted G7 RRM and partners for additional information		**MONITOR** LOW **GAC**: engagement or management of bilateral relations with responsible state via diplomatic channels
DEFEND LOW SIGINT **CSE** (CCCS): alert/advise victims, provide mitigation guidance, improve data/network integrity via engagement		**DISRUPT** LOW - HIGH **CSIS**: [redacted] via TRM process **CSE** (SIGINT): active cyber operation to degrade foreign actor's system or device **RCMP**: refer for prosecution if criminality established **GAC**: bilateral engagement with responsible state (e.g. calling in of Ambassador)		**EXPOSE** HIGH **GAC:** public attribution or demarche All SITE comms teams: strategic communication via third parties and/or media
DISRUPT LOW - MED **CSE** (CCCS): disrupt connection between foreign node and GoC/systems of importance infrastructure **RCMP**: refer for prosecution if criminality established				
EXPOSE MED **CSE** (CCCS)/**GAC:** via deconfliction and GAC public attribution framework **GAC**: strategic communication via third parties and/or media		**EXPOSE** HIGH **GAC:** public attribution or demarche All SITE comms teams: strategic communication via third parties and/or media		

Risk level
LOW MED HIGH

Risk is defined as reputational risk to the Government of Canada which includes, amongst other things, the perception of bias, ineffectiveness and overstepping the respective authorities of SITE TF agencies.

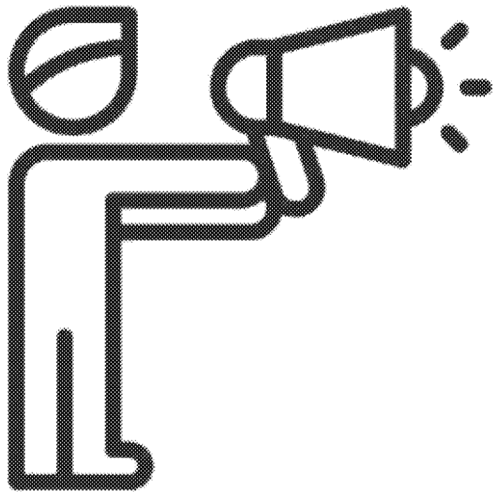
Canada

SITE TF Response Assumptions



- SITE TF agencies agree that as individual agencies, we all have independent mandates and authorities and are individually accountable for taking action pursuant to these mandates to protect the Canada's democratic institutions.
- As a community, SITE agencies also agree that we must maintain mutual awareness of one another's actions, and advise/de-conflict at the appropriate levels when required.
- What does this mean? SITE agencies agree to:
  - Ensure consistent and timely dissemination of all relevant intelligence to SITE TF members.
  - Operational approvals will remain unchanged during the writ period, and continue to reside with each agency. However, we commit to inform, consult and coordinate amongst SITE TF members on activities that deal with the 2019 federal election prior to taking action.
  - Maintain mutual awareness of intelligence briefed to Ministers as it specifically concerns the 2019 federal election.
  - SITE commits to ensuring that ADMs and DMs, including the panel, will be apprised of through a SITREP that will be disseminated daily. This will include intelligence and any considerations relating to ongoing or potential response actions

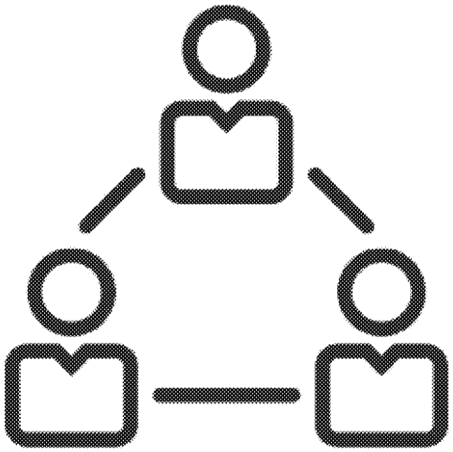
SITE TF Situation Report (SITREP)



Enhancing Communications

- Recognizing the need for increased communications before and during the writ period, SITE has developed a standardized SITREP.
- Formalizing SITE's weekly update to ADMs, the SITREP will be sent weekly, and potentially daily, to SITE TF ADMs, DMs and the Panel of 5.
- The SITREP will include SITE's assessment of the overall threat level, current threat updates and current operational updates.

SITE TF Surge Posture



- SITE TF members have developed their own internal surge postures in advance of the writs being issued.
- Operations Centres have received briefings from SITE TF members, informing them of their respective roles and responsibilities in the SITE TF Communications Protocols.
- A high-level overview of members surge postures is enclosed on the following slide.

SITE Surge Posture

TS/[redacted]/CEO

SITE internal engagement during writ period:
SITE daily phone updates (low-side or CTSN) + in-person meeting once a week

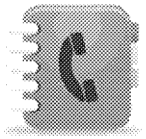
CSE	CSIS	GAC	RCMP
• SITE members: 24/7 on call from Sep 3–Oct 22 • CCCS: – On call 24/7 from Oct 11–20 – 24-hr support on site at CSE on polling day	• SITE members: 24/7 on call one week before and after writ drops • IAB technical and operational reporting: 48-hr turnaround	• SITE members: 24/7 on call from Sep 3–Oct 25	• NOC: 16/7 once writ drops

There are two main methods to contact SITE during **off hours and/emergencies**:

METHOD 1 – via SITE official email

- [redacted]
- Unclassified: site-tf@cyber.gc.ca

**A SITE TF rep will acknowledge the request, triage and advise rest of SITE.*

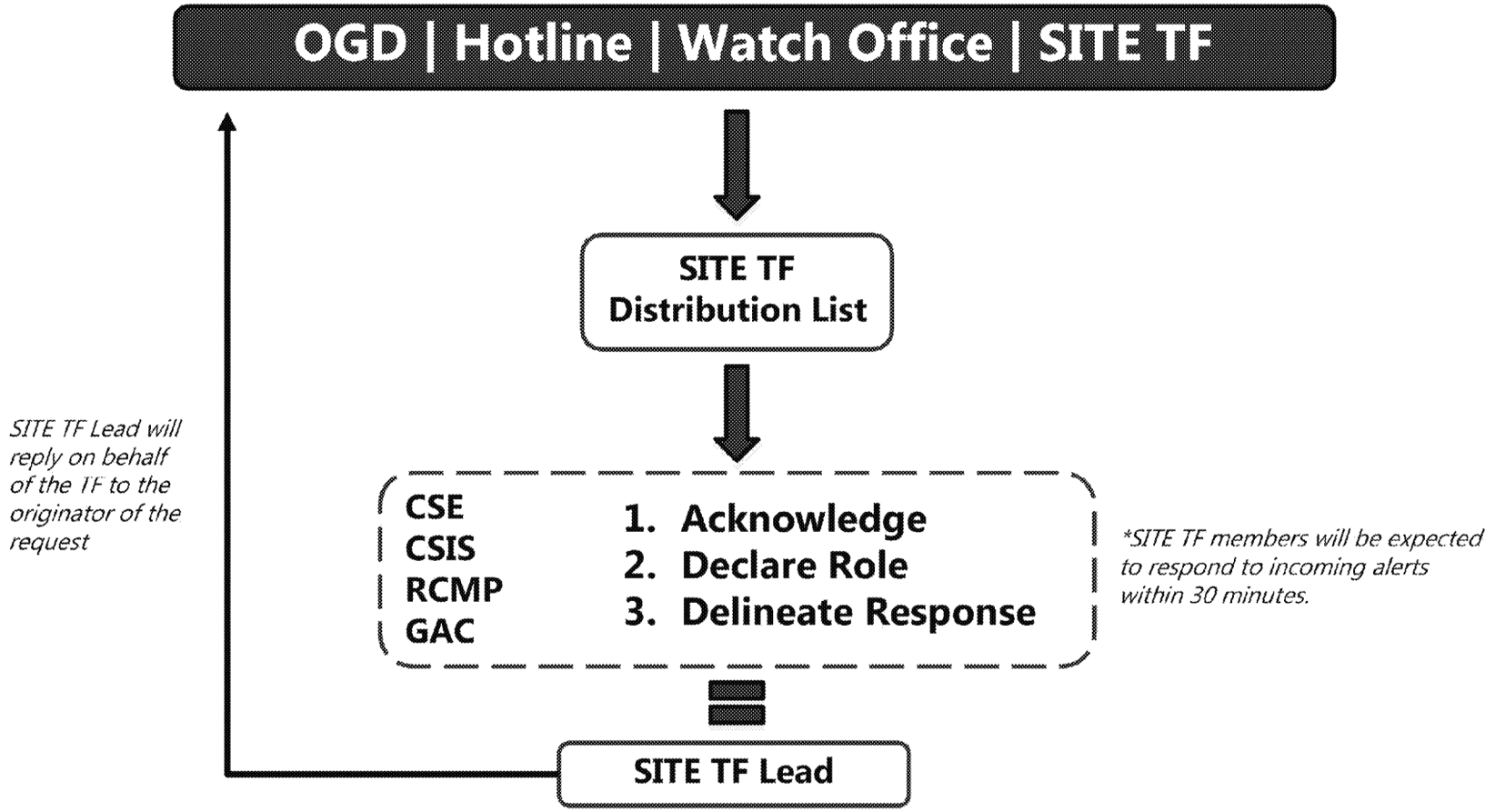


METHOD 2 – direct to respective SITE agencies

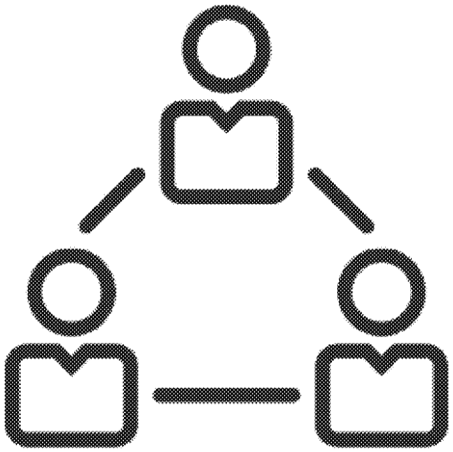
CSE Operational Production and Coordination Centre (COPCC) – 24/7	**CSIS** Global Operations Centre (CGOC) – 24/7	**GAC** Emergency Watch Centre – 24/7	**RCMP** NOC – 16/7
[redacted] unclass: copcc-osoc@cse-cst.gc.ca; 613-991-8762	[redacted] unclass: cgocalert@smtp.gc.ca 1-800-267-7685 613-993-9620	unclass: watchunit.csw@international.gc.ca	

Off-Hours 'Hotline' Call

TS/ /CEO



Engagements



Previous Engagements:

- SECRET-level call with political parties – August 21
- Minister of Democratic Institutions brief – August 23
- Visit from Singapore's Ministry of Home Affairs – August 29