



OPS-1-15

Operational Procedures for Cyber Defence Activities Using System Owner Data

OPERATIONAL POLICY

Canada

Table of Contents

1. Introduction	2
Policy Scope and Application	2
Activity Description	3
Legal Framework	3
2. Preparing for DPSO Activities	6
Pre-Requirements	6
3. Handling Raw System Owner Data	7
4. Cyber Defence Reports	9
Writing and Releasing Reports	9
Post-Publication Requests	9
5. Rules for Sharing Raw (Unreported) System Owner Data or Cyber Defence Report	10
6. Retention and Disposition Schedules	13
7. Roles and Responsibilities	14
8. Information about These Procedures	16
9. Definitions	17

1. Introduction

Policy Scope and Application

1.1 Scope

These procedures govern IT Security's (ITS) cyber defence activities using data provided by a system owner ("DPSO activities"). ITS does not intercept data for these activities, so a Ministerial Authorization (MA) is not required.



FYI: Throughout these procedures, the term "private communication" means an intercepted private communication. See paragraph 1.8.

1.2 Objective

These procedures:

- define mandatory measures to protect the privacy of Canadians during DPSO activities, and
- provide direction regarding
 - preparing for these activities
 - handling raw (that is, unreported) system owner data
 - writing and releasing CSEC cyber defence reports, and handling post-publication requests
 - sharing raw system owner data and cyber defence reports with SIGINT and outside of CSEC, and
 - applying retention and disposition schedules.

1.3 Policy

DPSO activities must:

- comply with the relevant laws of Canada, including the *Criminal Code*, the *Financial Administration Act*, the *Privacy Act*, and the *National Defence Act* (NDA)
- comply with all relevant Ministerial Directives, including the *Ministerial Directive on the Privacy of Canadians* and the *Ministerial Directive on CSE's Accountability Framework* (both June 2001)
- adhere to any conditions set out by the entity receiving ITS' help
- be subject to measures to protect the privacy of Canadians, including those prescribed in OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- comply with these procedures, as well as other related IT Security policy instruments and documentation

Continued on next page

1.3 Policy
(continued)

- be carried out only with the knowledge and approval of CSEC management and the management of the entity receiving ITS's help
- be subject to internal CSEC monitoring for policy compliance, and
- be subject to audit or review by various government review bodies, including, but not limited to, the CSE Commissioner and the Privacy Commissioner.

1.4 Application

These procedures apply to CSEC personnel and any other parties, including secondees, contractors and intregrees, who are involved in or make use of data from DPSO activities.

Activity Description

1.5 What are DPSO activities?

DPSO activities are meant to address perceived cyber threats against computer systems or networks, and all of the electronic information contained in them. These systems are owned or controlled by the Government of Canada (GC) or by non-GC entities whose systems are of importance to the GC.

ITS undertakes DPSO activities when a system owner or a GC intermediary such as Public Safety, who may have been approached by a system owner for mitigation assistance, requests ITS's help. ITS relies on the requestor to provide data from the owner's systems. ITS staff analyzes this data to detect and mitigate the perceived cyber threat.



Note: Throughout these procedures, the term "requestor" is used to describe the entity that formally requests and receives ITS' help.

Legal Framework

1.6 Authority to allow ITS Analysis of System Owner Data


Paragraph 273.64(1)(b) of the NDA (part (b) of the CSEC mandate) gives ITS the authority to "provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the GC".

This means that, in addition to supporting GC departments, ITS may also help non-GC entities whose systems are deemed to be of importance to the GC.

1.7 What is a Private Communication?

Section 183 of the *Criminal Codes* defines a private communication as “any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it”.

A communication must be intercepted while *in transit* to be considered a private communication under Part VI of the *Criminal Code*.



Note: The legal distinction between “data at rest” and “data in transit” in relation to the interception of a private communication can be complex. When in doubt, contact ITS Policy Oversight and Compliance (IPOC) for guidance on what is considered to be a private communication.

1.8 Interception of a Private Communication by a System Owner

Two legal provisions permit the lawful interception of a private communication by a system owner.

Paragraph 184(2)(e) of the *Criminal Code* provides an exemption from criminal liability for persons who perform duties related to the management or protection of computer systems (that is, system owners) who may intercept a private communication if the interception is necessary for such purposes.

Under section 161 of the *Financial Administration Act* (FAA), those responsible for managing or protecting GC computer systems or networks are authorized to take measures, including intercepting a private communication, if the interception is necessary for such purposes.

1.9 Disclosure of a Private Communication to ITS by a System Owner

In accordance with section 193 of the *Criminal Code*, a system owner may disclose to ITS (either directly or through a GC intermediary) all or part of a private communication, but only if the disclosure is necessary to protecting or managing the owner’s computer systems (to help mitigate the cyber threat affecting the owner’s computer systems).

1.10 Sharing a Private Communication by ITS

When undertaking DPSO activities, ITS may obtain a private communication that was acquired from an owner's computer systems. *Criminal Code* provisions allow ITS to share this private communication with SIGINT or outside of CSEC as outlined below (express requestor consent must be obtained).

1. ITS, on behalf of the system owner, may share the private communication (for example, with SIGINT, another GC department or a Second Party), but only if this will help mitigate the cyber threat affecting the owner's computer systems.
2. ITS, on behalf of the system owner, may share the private communication with CSIS or the RCMP to allow those departments to fulfill their respective mandates.
3. With the consent of either the originator or the recipient of the private communication, ITS may share this communication in accordance with the given consent. Given the nature of system owner data, consent would most likely be obtained from the recipient (for example, the recipient of an email embedded with malicious code that was intercepted by that employee's information protection centre).



Note: Throughout these procedures, this third type is referred to as "a private communication with recipient consent" (originator consent, if applicable, is not precluded).

2. Preparing for DPSO Activities

Pre-Requirements

2.1 Documented Request ITS may only undertake DPSO activities when it receives a documented request for help from the requestor. The requestor may be a system owner or an appropriate representative of the system owner such as Public Safety, with the system owner consent.

2.2 Types of Information Requiring Privacy Protection Measures

The following two categories of information require privacy protection measures:

1. A private communication, and
2. Information about Canadians, which is defined as:
 - a. any personal information about a Canadian, or
 - b. any information about a Canadian corporation.

These categories of information must be protected by the use of access controls and by ITS senior management approval of reports as per OPS-1. Moreover, Canadian identity information (CII) must be protected in accordance with OPS-1-6, *Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports*.

2.3 CSEC's Personal Information Bank for Cyber Protection

To comply with its obligations under the *Privacy Act* regarding personal information, ITS must account for all personal information it retains while conducting DPSO activities. This information must be accounted for in CSEC's Personal Information Bank (PIB) for Cyber Protection.

ITS must not use personal information it has obtained during DPSO activities for administrative purposes.

3. Handling Raw System Owner Data

3.1 Introduction This section outlines the basic rules governing the handling of raw (that is, unreported) system owner data.



Note: Throughout these procedures, system owner data falls within one of these three categories:

- a private communication
- a private communication with recipient consent (see paragraph 1.10), or
- IRRELEVANT

Handling will be different for a private communication, a private communication with recipient consent, IRRELEVANT

3.2 Identifying a Private Communication The requestor determines whether the system owner data it provides to ITS includes a private communication and is essential to protecting the owner's systems. ITS will assist with this determination as necessary; however, ITS is not required to conduct an "essentiality test".

3.3 Labeling System owner data must be identified with a label. Labeling will ensure the proper application of retention and disposition schedules.

3.4 Classification At a minimum, system owner data must keep its original classification. The classification may be raised, for example if sensitive analytic capabilities could be revealed.

3.5 Access Permissions Access to system owner data must be strictly controlled and limited to staff within CSEC who are involved in or make use of data from DPSO activities or in accordance with the consent given.

3.6 Information Indicating a Criminal Offence

If, during DPSO activities, there are indications of a *Criminal Code* offence that is unrelated to a cyber threat, the incident must be brought to the attention of the relevant Director in the Cyber Defence Branch. The Director may seek advice from the Directorate of Legal Services (DLS), as needed, prior to informing the requestor, who has responsibility with respect to follow-on action. The Deputy Chief (DC) ITS must be notified of the incident.



Warning: All details concerning any such discovery must be controlled and shared on a strict "need-to-know" basis.

3.7 Dealing with Other Breaches

If, during DPSO activities, there are indications of a breach in a requester's policy that is unrelated to a Criminal Code offence or a cyber threat (for example, a security breach such as SECRET data being sent over an unclassified network), the incident must be brought to the attention of the relevant Director in the Cyber Defence Branch, who will consult with IPOC staff as necessary on what action should be taken.

3.8 Request for Suspension or Termination

ITS must stop all analysis upon receiving a request for suspension or termination of DPSO activities.

4. Cyber Defence Reports

Writing and Releasing Reports

4.1 Suppressing Identity Information

ITS must follow the “naming rules” set out in OPS-1-6 when Canadian identities will be reported.

US/UK/AUS/NZ identities are handled in accordance with their own national policies.



Note: Raw system owner data or cyber defence reports may be shared with SIGINT without suppression of CII. See Chapter 5.

4.2 Pre-approved Actions

Where applicable, cyber defence reports (including those that are disseminated to SIGINT) may set out actions that can be taken by the recipient without prior consultation with CSEC.

4.3 Report Release Authorities

Report Release Authorities must review and approve reports for release prior to dissemination as set out in OPS-1. In addition to ensuring that privacy measures have been properly applied, Report Release Authorities are responsible for ensuring that reports that may affect equities (for example, SIGINT equities) are identified, and that appropriate consultations are conducted prior to report release.

Post-Publication Requests

4.4 Releasing Identity Information

Operational Policy is the authority for releasing suppressed Canadian or US/UK/AUS/NZ identities, in accordance with OPS-1-6.



Warning: Anyone outside Operational Policy who releases identity information is committing a privacy violation.

4.5 Follow-on Action

Operational Policy must approve requests for follow-on action beyond any actions set out in the report caveat.

5. Rules for Sharing Raw (Unreported) System Owner Data or Cyber Defence Report

5.1 Principles

Requester consent must be obtained for sharing raw system owner data or cyber defence reports with SIGINT, CSIS and the RCMP, other GC departments or Second Parties and:

- Sharing must be in the proper exercise of part (b) of the CSEC mandate. This would include sharing with SIGINT provided that part (a) of the mandate includes cyber security foreign intelligence activities and as such, this sharing would be in line with part (b) of the CSEC mandate.
- A private communication must only be shared to help mitigate the cyber threat affecting the system owner (CSIS and the RCMP may use the private communication more widely, but within their mandate).
- All sharing of raw system owner data must be approved by the relevant Manager in the Cyber Defence Branch.

5.2 Sharing Rules Table

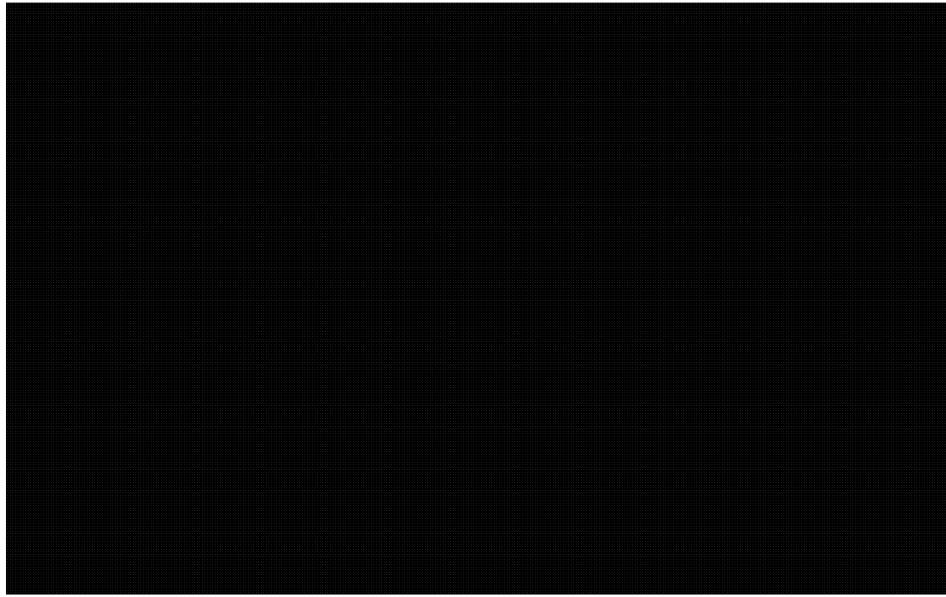
The following table sets out the rules for sharing raw system owner data and cyber defence reports with SIGINT, CSIS and the RCMP, or other GC departments or Second Parties.

Continued on next page

SECRET
OPS-1-15
Effective Date: 25 January 2012

	Is sharing permissible with...	for private communications?	for private communications with express recipient consent?	for other data?
Raw (Unreported)	SIGINT	Yes, but only for triaging (see paragraph 5.3), or to help mitigate the cyber threat affecting the system owner (suppression of CII not required)	Yes for cyber-security foreign intelligence activities (suppression of CII not required), as long as not precluded by consent given	Yes, for cyber-security foreign intelligence activities (suppression of CII not required)
	CSIS and RCMP	Yes, to fulfill their respective mandates (express system owner consent required and suppression of CII not required)	Yes, to fulfill their respective mandates (suppression of CII not required)	
	Other GC Departments or Second Parties	No (must be reported)	No (must be reported)	
Reported	SIGINT	Yes, but <u>only</u> to help mitigate the cyber threat affecting the system owner (suppression of CII not required)	Yes, for cyber-security foreign intelligence activities (suppression of CII not required), as long as not precluded by consent given	Yes, for cyber-security foreign intelligence activities (suppression of CII not required)
	CSIS and RCMP	Yes	Yes	
	Other GC Departments or Second Parties	Yes, but <u>only</u> to those involved in the provision of protective measures to help mitigate the cyber threat affecting the system owner	Yes, as long as not precluded by consent given	Yes, or as per requestor consent

5.3
Clarifications
for Sharing with
SIGINT



6. Retention and Disposition Schedules

- | | |
|----------------------------------|--|
| 6.1 Application | ITS must apply retention or disposition schedules to all system owner data, regardless of media or location (e.g. hard copy, personal or group accounts, or electronic repositories). |
| <hr/> | |
| 6.2 Cyber Defence Reports | Cyber defence reports must be retained or destroyed in accordance with CSEC-approved retention and destruction schedules. Private communications or other data that are included in a report must be retained with the corresponding report. |
| <hr/> | |
| 6.3 Raw System Owner Data | <p>Upon termination of a DPSO activity, ITS</p> <ul style="list-style-type: none">• may retain system owner data if the requestor has approved its retention and it is relevant to providing advice and guidance to protect IT systems of importance to the GC, and• will delete all non-relevant system owner data as well as system owner data the requestor has not approved retention of within [REDACTED] after termination of DPSO activity |
-

7. Roles and Responsibilities

7.1 Roles and Responsibilities This table describes the key roles and responsibilities with respect to cyber event support activities.

Who	Roles and Responsibilities
Deputy Chief, IT Security	<ul style="list-style-type: none"> Accounting for all DPSO activities Acting as Release Authority for reports Seeking legal advice, as required
Directorate, Legal Service	<ul style="list-style-type: none"> Providing legal advice, including legal briefings, when required
Director General, Cyber Defence	<ul style="list-style-type: none"> Acting as Recommend Authority for reports Seeking legal advice, as required
Director, Cyber Defence Operations and Capabilities Development	<ul style="list-style-type: none"> Acting as Recommend Authority for reports Seeking legal advice, as required Ensuring compliance with these procedures
Director, Program Management and Oversight (PMO)	<ul style="list-style-type: none"> Coordinating the resolution of policy and legal issues Coordinating the conduct and implementation of recommendations from internal and external reviews Seeking legal advice, as required
Director, Cyber Threat Evaluation Centre (CTEC)	<ul style="list-style-type: none"> Acting as Recommend or Release Authority for reports Seeking legal advice, as required Ensuring compliance with these procedures
Director, Corporate and Operational Policy	<ul style="list-style-type: none"> Seeking legal advice, as required
Managers in the Cyber Defence Branch	<ul style="list-style-type: none"> Ensuring that staff involved in DPSO activities comply with any conditions set out in writing by the requestor, and all relevant policy instruments Acting as Release Authority for reports Raising legal and policy concerns with the relevant Director in the Cyber Defence Branch
Manager, Operational Policy	<ul style="list-style-type: none"> Managing the review and approval of follow-on action requests Providing support to ensure consistency in policy advice, as required
Manager, External Review	<ul style="list-style-type: none"> Leading CSEC's response to external reviews
ITS Policy Oversight and Compliance (IPOC)	<ul style="list-style-type: none"> Providing policy advice to staff involved in DPSO activities

Effective Date: 25 January 2012

Who	Roles and Responsibilities
Operational Supervisors in the Cyber Defence Branch	<ul style="list-style-type: none"> • Providing technical direction and guidance to staff involved in DPSO activities • Acting as Recommend Authority for reports • Ensuring that system owner data has been destroyed in accordance with these procedures • Complying with the requestor's instructions and all relevant policy instruments and documentation
Staff involved in DPSO activities	<ul style="list-style-type: none"> • Complying with the requestor's instructions and all relevant policy instruments and documentation • Destroying system owner data in accordance with these procedures

8. Information about These Procedures

- 8.1 Accountability** This table outlines accountabilities for revising, reviewing, recommending and approving these procedures.

Who	What
Deputy Chief, IT Security	Approving these procedures
Director General, Policy and Communications	Recommending these procedures for approval
General Counsel, Directorate of Legal Services	<ul style="list-style-type: none">• Reviewing these procedures and advising on their compliance with the law• Providing legal advice when requested
Director, COP	Reviewing these procedures and advising consistency within the policy framework
Operational Policy	Revising these procedures

- 8.2 References**
- *National Defence Act*, part V.1
 - *Privacy Act*
 - *Criminal Code*
 - *Financial Administration Act*
 - *Library and Archives of Canada Act*
 - *Ministerial Directive on the Privacy of Canadians*, June 2001
 - *Ministerial Directive on CSEC's Accountability Framework*, June 2001
 - OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
 - OPS-1-6, *Procedures for Naming and Releasing Identities from Cyber Defence Reports*

- 8.3 Amendment Process** Situations may arise where amendments to these procedures are required because of changing or unforeseen circumstances. Such amendments will be communicated to relevant staff and will be posted on the Operational Policy website.

- 8.4 Enquiries** Questions related to these procedures must be addressed to operational managers, who in turn will contact IPOC staff. IPOC will consult Operational Policy, as required.

9. Definitions

9.1 Canadian

“Canadian” refers to

- a) A Canadian citizen, or
- b) A person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act* (IRPA), and who has not subsequently lost that status under that *Act*, or
- c) A corporation incorporated under an Act of Parliament or of the legislature of a province.

(NDA, section 273.61; IRPA)

For the purpose of these procedures, “Canadian organizations” are accorded the same protection as Canadian citizens and corporations.

A Canadian organization is an unincorporated association, such as a political party, a religious group, or an unincorporated business headquartered in Canada.

9.2 Canadian Identity Information (CII)

Canadian Identity Information (CII) refers to information that may be used to identify a Canadian person, organization, or corporation, including, but not limited to names, phone numbers, email addresses, IP addresses, and passport numbers.



Reminder: Raw system owner data or cyber defence reports may be shared with SIGINT without suppression of CII.

9.3 Cyber Defence Reports

Reports may serve a variety of purposes, including (but not limited to):

- reporting suspicious activity
- exchanging information
- reporting incidents
- sharing detection capabilities (e.g. tools or signatures)
- providing analysis
- sharing malicious code and associated analysis
- showing trends, and
- providing situational awareness.

Report formats may vary and can include a variety of vehicles, such as formalized reporting and data sharing by email.

9.4 DPSO Activities	DPSO activities are carried out by ITS using data provided by system owners (either directly or through a GC intermediary). They are meant to address perceived cyber threats against computer systems or networks, and all of the electronic information contained in them. These systems are owned or controlled by the Government of Canada (GC) or by non-GC entities whose systems are of importance to the GC.
9.5 Follow-on Action	Any action, or decision to act, taken by the recipient of a CSEC cyber defence report on the basis of the reported information beyond any actions set out in the report caveat.
9.6 Information about Canadians	Information about Canadians refers to: <ul style="list-style-type: none"> • any personal information about a Canadian, or • any information about a Canadian corporation.
9.7 Integree	An integree is a person seconded to CSEC from one of CSEC's cryptologic partner organizations.
9.8 Ministerial Authorization	<p>A Ministerial Authorization (MA) is an authorization provided in writing by the Minister of National Defence to CSEC to ensure that CSEC is not in contravention of the law if, in the process of conducting its foreign intelligence or IT security operations, it should intercept private communications. MAs may be granted in relation to an activity or class of activities specified in the authorization pursuant to</p> <ul style="list-style-type: none"> • subsection 273.65(1) of the NDA for the sole purpose of obtaining foreign intelligence, or • subsection 273.65(3) of the NDA for the sole purpose of protecting the computer systems or networks of the GC. <p>When such an authorization is in force, Part VI of the <i>Criminal Code</i> does not apply in relation to an interception of a private communication, or in relation to a communication so intercepted.</p>
9.9 Personal Information	Personal information is defined in the <i>Privacy Act</i> as "information about an identifiable individual that is recorded in any form". See OPS-1, Annex 1 for the complete definition.

9.10 Personal Information Bank (PIB)	<p>The legal obligation to establish a PIB is set out in subsection 10(1) of the <i>Privacy Act</i>, which states that the head of a government institution shall cause to be included in personal information banks all personal information under the control of the government institution that</p> <ul style="list-style-type: none"> (a) has been used, is being used or is available for use for an administrative purpose; or (b) is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.
9.11 Private Communication	<p>A private communication is “any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.” (<i>Criminal Code</i>, section 183)</p>
9.12 Retention Schedules	<p>The time allotted for retaining a record or specific types of records within an organization. Retention schedules reflect all legal, policy and operational requirements levied against an organization and its holdings.</p>
9.13 Requestor	<p>The requestor is entity that requests and receives ITS’ help. The requestor may be a system owner, or a GC intermediary who is an appropriate representative of the system owner such as Public Safety.</p>
9.14 Second Parties	<p>Second Parties refers to CSEC’s counterparts: the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), Australia’s Defence Signals Directorate (DSD), and New Zealand’s Government Communications Security Bureau (GCSB).</p>
9.15 Seconded	<p>A secondee is an individual who is temporarily moved from another GC or private organization to CSEC, and who at the end of the assignment returns to the originating organization.</p>

9.16 Suppressed Information	<p>Suppressed information is defined as information excluded from a SIGINT end product or technical report or an IT Security report because it may reveal the identity of a Canadian or US/UK/AUS/NZ entity. Suppressed information is stored in a limited access database or system and is replaced in the report by a generic term.</p> <p>Suppressed information includes, but is not limited to, personal identifiers such as names, passport information, [REDACTED] email addresses, phone numbers and IP addresses. [REDACTED] [REDACTED]</p>
9.17 System Owner	<p>A system owner is the entity that owns or controls GC or non-GC computer systems or networks, and all of the electronic information contained in them.</p>
9.18 System Owner Data	<p>System owner data is data that is obtained from the system owner's computer systems or networks. It may include a private communication, a private communication with recipient consent, or other data.</p>
9.19 Triaging	<p>Refers to sharing raw private communications with SIGINT to help determine the operational significance of this data on condition that SIGINT not use or retain this data for foreign intelligence purposes (that is, part (a) of the CSEC mandate).</p>
