Outstanding OCSEC Recommendations

#	Review #	Review - Short Title	Review - Full Title	Review Recommendations	CSE Management Response	Current Status	Business Line Responsible	Group responsible	Expected Completion Date	Status	CSE Comments (for Internal Use)	CSE Comments (for External Use)
2	90	SIGINT Metadata	Review of CSE Use of Metadata in a SIGINT Context	Recommendation no. 2: CSE should use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization.	Recommendation accepted. Improved record-keeping relating to changes to collection systems and minimization protocols will be included in the corrective actions being undertaken by SIGINT to address the problems identified with the automated sharing of metadata with the Second Parties. CSE expects to complete this process by the end of fiscal year 2015-2016.		SIGINT	SPR	Q4 2015-2016	In Progress	**Aug 2015**: D3 [redacted] to discuss with SPR on next steps (issuing guidance or developing standards, etc.) **Oct 2015:** SPI 7-14 originally issued in Sep 2014, and revised in Jan 2015 provides specific instructions regarding roles, responsibilities and documentation required when changes are made to any minimization process. There is a web form that is supposed to be completed whenever a change is made but I'm still tracking down who that form goes to and what they do with it. According to [redacted] SPR Compliance Team Manager, [redacted] in [redacted] is currently working to ensure all relevant documentation to the DNR minimization effort is captured in the corporate repository but she is unaware of the web form. I'll need to check if correspondence relating to DNI minimization is also being addressed by [redacted] are both away until 2 Nov 2015.	
1	90	SIGINT Metadata	Review of CSE Use of Metadata in a SIGINT Context	Recommendation no. 1: CSE should seek an updated Ministerial Directive that provides clear guidance related to the collection, use and disclosure of metadata.	Recommendation accepted. CSE will support the Minister in the development of an updated Ministerial Directive to provide guidance related to the collection, use and disclosure of metadata. CSE expects to have a Ministerial Directive proposal package ready for the Minister's consideration by the end of fiscal year 2015-2016.		DGPC	B	Q4 2015-2016	In Progress	**Aug 2015**: D3 to discuss with B group in upcoming bilat	
2	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2012	Recommendation no. 2: Cyber Defence Operations Private Communications CSE reporting to the Minister of National Defence on private communications unintentionally intercepted under ministerial authorizations should highlight the important differences between one-end in Canada e-mails intercepted under cyber defence operations and private communications intercepted under foreign signals intelligence activities, including the lower expectation of privacy attached to the private communications intercepted under cyber defence operations.	Accepted: CSE will provide additional information in its upcoming annual report that will highlight the difference between private communications intercepted under cyber defence and the foreign intelligence operations. This supplemental reporting will begin with next year's Annual Report.		ITS / DGPC	B	Q3 2015-2016	In Progress	**Aug 2015**: D3 reminded B and ITS of recommendation for consideration in upcoming MA report. Topic to be further discussed in upcoming D3-B Bilat. **Oct 2015**: The draft MA Year End report does highlight how ITS PCs differ under the "Total PC retained" table.	
1	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2012	Recommendation no. 1: Subsection 273.65(3) of the National Defence Act CSE should encourage the government to amend subsection 273.65(3) of the National Defence Act as soon as practicable to remove any ambiguities respecting CSE's authority to conduct IT security activities that risk the interception of private communications.	Accepted: Subject to the Minister's discretion, CSE will support the Minister in identifying potential changes to legislation that address the ambiguities identified by the CSE Commissioner in this review.		DGPC	B	Q2 2015-2016	In Progress	**Aug 2015**: Topic to be further discussed in upcoming D3-B Bilat	

#	Review #	Review - Short Title	Review - Full Title	Review Recommendations	CSE Management Response	Current Status	Business Line Responsible	Group responsible	Expected Completion Date	Status	CSE Comments (for Internal Use)	CSE Comments (for External Use)
4	IRRELEVANT											
3												
2												
1												
2	79	Office of Counter Terrorism 2012	Review of the Actitivies of the Office of Counter Terrorism 2012	Recommendation 2: CSE should promulgate guidance to codify its practices to address cases when an analyst identifies that a Second Party is targeting a Canadian, including notification to the Second Party to desist from such targeting and recod keeping of such cases.	CSE will develop and promulgate guidance regarding the procedures that analysts should follow, if they determine a Canadian is being targeted by a Second Party. This will include requesting that the Second Party cease its targeting.	**OUTSTANDING**	DGPC	D2A	Q1 2015-2016	In Progress	IRRELEVANT **Sept 2015**: SPR will be issuing guidance, not D2.	
5	75	SIGINT MAs 2013	Review of CSEC's 2013 Foreign Signals Intelligence Ministerial Authorizations	Recommendation 2: CSE should make available to the Minister more comprehensive information regarding the number of intercepted communications and intercepted private communications that it acquires and retains throughout an MA period, in order to enhance accountability to the Minister	CSE will include more information in the 2014-2015 MA annual report, regarding the fluctuations in numbers of retained PCs throughout the reporting year.	**OUTSTANDING**	DGPC/SIGINT	B/SPOC	2014-2015	In progress	Recommendation was partially satisfied by providing additional context in the recent MA report. B group and SIGINT continuing discussions to enhance information to be captured in future MA reports. **April** 2015: SPR2 and B group have had discussions and will continue to refine implementation. The status continues to be "in progress". SPR2 anticipates producing a mock-up for further discussion with B group (probably in June, as preparation for the next MA request memos [November], based on a monthly pull of the MA stats) that will inform what the year-end report could look like. **October 2015:** The draft MA Year End Report (in progress) contains an additional Annex (Annex A) that provides a month-by-month break down of retained SIGINT PCs.	CSE has partially satisfied this recommendation by providing in the 2013-14 MA Year End Report, more comprehensive information regarding the number of SIGINT PCs retained throughout the reporting period. Technical developments will continue in order to provide the Minister (in the 2014-15 MA Year End report) with more detailed information regarding the fluctuations in numbers of retained SIGINT PCs throughout the reporting period. **(April 2015)**
8	75	SIGINT MAs 2013	Review of CSEC's 2013 Foreign Signals Intelligence Ministerial Authorizations	Recommendation 5: CSE should promulgate guidance regarding the treatment of [redacted] acquired as part of [redacted] collection, but which [redacted] constituted a private communication or a two-end Canadian communication.	Recommendation accepted with modifications. CSE will promulgate guidance by Q2.	**OUTSTANDING**	DGPC/SIGINT	D2B/SPOC	KEY SCENARIOS Q3 - RELATED GUIDANCE Q4	In Progress	2014: Initial timeline delayed - Scenarios still in development ; 2015: The recommendation related to a very specific set of circumstances that arose in the review. Responsibility for implementation will rest with SPR1. **Aug 2015**: D3 [redacted] to discuss with SPR and D2. **OCT 2015:** Met with SPR to discuss the way forward on this. [redacted] and DGI will provide specific scenarios to SPR SIGINT Policy who will write guidance to cover these specific situations. It is planned that when complete this guidance will be emailed to DGI teams and also added to SPR's [redacted] page.	In FY 14-15, priority was placed on implementing solutions to address recommendations 3 and 4, and to updating CSOI-4-3. SPR will address the recommendation and implement guidance by the close of Q3. **(April 2015)**

#	Review #	Review - Short Title	Review - Full Title	Review Recommendations	CSE Management Response	Current Status	Business Line Responsible	Group responsible	Expected Completion Date	Status	CSE Comments (for Internal Use)	CSE Comments (for External Use)
10	74	Second Party Info Sharing	A Review of CSEC SIGINT Information Sharing with the Second Parties	Recommendation 2: To support the Minister of National Defence in his accountability for CSEC and as a measure to protect the privacy of Canadians, it is recommended that the Minister issue, under his authority pursuant to subsection 273.62(3) of the National Defence Act, a new ministerial directive to provide general direction to CSEC on its foreign signals intelligence information sharing activities with its Second Party partners in the United States, United Kingdom, Australia and New Zealand, and to set out expectations for the protection of the privacy of Canadians in the conduct of those activities.	CSE will support the Minister in the development of a new ministerial directive to provide general direction to CSE on its information sharing activities with its Second Party partners, with a focus on privacy and legal obligations associated with such information sharing. CSE will begin undertaking the necessary preparatory work that will inform the development of a proposal package for an MD that will apply to both SIGINT and IT Security, and will address the following points: • The history and value of CSE's information sharing arrangements with Second Parties; • Canada's expectations from the Five-Eyes information sharing arrangements; • Limits on information sharing and measures to protect the privacy of Canadians; • Requirements for reporting to the Minister; • Compliance monitoring; and • Review by the CSE Commissioner CSE expects that an MD proposal submission will be provided to the Minister for consideration by the end of fiscal year 2014/2015.	OUTSTANDING	DGPC	B / D2	2014/2015	In Progress	2014: MD and related Risk Assessment have been drafted but require CSE senior management approvals. **Aug 2015**: MD and related Risk Assessment awaiting senior management approval	

#	Review #	Review - Short Title	Review - Full Title	Review Recommendations	CSE Management Response	Current Status	Business Line Responsible	Group responsible	Expected Completion Date	Status	CSE Comments (for Internal Use)	CSE Comments (for External Use)
11	IRRELEVANT											
12												
13												

	Number of Reviews			
	SIGINT	ITS	Corporate	Total
1 April 1996 - 31 March 1997	1	0	0	1
1 April 1997 - 31 March 1998	1	0	2	3
1 April 1998 - 31 March 1999	1	0	0	1
1 April 1999 - 31 March 2000	3	1	1	5
1 April 2000 - 31 March 2001	2	1	2	5
1 April 2001 - 31 March 2002	3	1	0	4
1 April 2002 - 31 March 2003	3	1	0	4
1 April 2003 - 31 March 2004	2	2	1	5
1 April 2004- 31 March 2005	4	1	0	5
1 April 2005- 31 March 2006	2	1	0	3
1 April 2006- 31 March 2007	3	1	0	4
1 April 2007- 31 March 2008	4	0	0	4
1 April 2008- 31 March 2009	6	0	1	7
1 April 2009- 31 March 2010	2	1	1	4
1 April 2010 - 31 March 2011	3	2	1	6
1 April 2011 - 31 March 2012	3	0	4	7
1 April 2012- 31 March 2013	3	1	2	6
1 April 2013- 31 March 2014	5	0	2	7
1 April 2014- 31 March 2015	6	1	2	9
	57	14	19	90
	63.3%	15.6%	21.1%	

	Number of Recommendations							Recommendations Status		
SIGINT	ITS	Corporate	Total	Not accepted	Rec. made by OCSEC to OCSEC	CSE Accountable	Completed	On Track	Overdue
2	0	0	2	0	0	2	2	0	0
2	0	2	4	0	0	4	4	0	0
1	0	0	1	0	0	1	1	0	0
1	2	0	3	0	0	3	3	0	0
1	1	4	6	0	1	6	6	0	0
9	4	0	13	1	0	12	12	0	0
13	3	0	16	0	0	16	16	0	0
0	4	11	15	0	0	15	15	0	0
21	0	0	21	6	2	13	13	0	0
8	5	0	13	0	0	13	13	0	0
9	5	0	14	0	0	14	14	0	0
9	0	0	9	1	0	8	8	0	0
13	0	0	13	0	0	13	10	0	3
1	0	2	3	0	0	3	3	0	0
4	0	0	4	2	0	2	2	0	0
0	0	0	0	0	0	0	0	0	0
3	0	1	4	0	0	4	4	0	0
4	0	6	10	0	0	10	6	4	0
2	1	5	8	0	0	8	0	8	0
103	25	31	159	10	3	147	132	12	3
64.8%	15.7%	19.5%		6.60%	2%	92.45%	89.80%	8.16%	2.04%

Total Reviews conducted to date	90		Total recommendations to CSE	159	
SIGINT reviews account for	63.3%	of total reviews	SIGINT recommendations account for	103	64.8% of total recommendations
ITS reviews account for	15.6%	of total reviews	ITS recommendations account for	25	15.7% of total recommendations
Total Actionable Recommendations to date			147		
Percentage completed			89.80%		
Percentage on track			8.16%		
Percentage overdue			2.04%		

Review Number	Recommendation Number	Review Short Title (Max 15 Char)	Review - Full Title	Review Recommendations	Review Category	Review Original Due Date to the End of FY	Recommendation Accepted (Yes/No)	CSEC Management Response	Review Lead Responsible	Review Lead Organization	Due Date	Actual Completion Date	Status	CSEC Comments (if required)	CSEC Comments (if required)	Review Updated? (Yes)
91		[redacted] Review	Review of CSEC [redacted] Activities [redacted] Interception) under Foreign Signals Intelligence Ministerial Authorizations													
90	2	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Recommendation no. 2: CSE should use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization.	Process	March 31 2015	Accepted	Recommendation accepted. Improved record-keeping relating to changes to collection systems and minimization protocols will be included in the corrective actions being undertaken by SIGINT to address the problems identified with the automated sharing of metadata with the Second Parties. CSE expects to implement these corrective actions by the end of fiscal year 2015/2016.	SIGINT	SPOC	Q4 2015-2016					
90	1	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Recommendation no. 1: CSE should seek an updated Ministerial Directive that provides clear guidance related to the collection, use and disclosure of metadata.	Authorities	March 31 2015	Accepted	Recommendation accepted. CSE will support the Minister in the development of an updated ministerial directive to provide guidance related to the collection, use and disclosure of metadata. CSE expects that a draft ministerial directive package will be provided to the Minister for consideration by the end of fiscal year 2015/2016.	DGPC	B	Q4 2015-2016					
89	2	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2012	Recommendation no. 2: Cyber Defence Operations Private Communications CSE reporting to the Minister of National Defence on private communications unintentionally intercepted under ministerial authorizations should highlight the important differences between one-end in Canada e-mails intercepted under cyber defence operations and private communications intercepted under foreign signals intelligence activities, including the lower expectation of privacy attached to the private communications intercepted under cyber defence operations.	Authorities	April 8 2015	Accepted	CSE will provide additional information in its upcoming annual report that will highlight the difference between private communications intercepted under cyber defence and the foreign intelligence operations.	ITS and DGPC	B	Q3 2015-2016					
89	1	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2012	Recommendation no. 1: Subsection 273.65(3) of the National Defence Act CSE should encourage the government to amend subsection 273.65(3) of the National Defence Act as soon as practicable to remove any ambiguities respecting CSE's authority to conduct IT security activities that risk the interception of private communications.	Legal ("Update/clarify certain instruments")	April 8 2015	Accepted	CSE will provide information to the Minister outlining the changes necessary to remove the ambiguities.	DGPC	B	Q2 2015-2016					
88	0	PIF and MPER 2014	Annual review of the Communications Security Establishment (CSE) Privacy Incident File (PIF) and Minor Procedural Errors Report (MPER) for calendary year 2014	No recommendations	n/a	March-31-15	N/A	N/A	N/A	N/A	N/A	N/A	N/A			
87	0	Disclosures 2014	Annual review of disclosures, by the Communications Security Establishment (CSE), of Canadian identity information (CII) from CSE end-product reports disseminated to clients	No recommendations	n/a	March-12-15	N/A	N/A	N/A	N/A	N/A	N/A	N/A			
86	0	SIGINT MAs	Annual Combined Review of Foreign Signals Intelligence Ministerial Authorizations for 2013-2014	No recommendations	n/a	March-03-15	N/A	N/A	N/A	N/A	N/A	N/A	N/A			
85	0	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	No recommendations	n/a	March 19 2015	N/A	N/A	N/A	N/A	N/A	N/A	N/A			
84		IRRELEVANT														
84																
84																

Review Number	Recommendation #	Review - Short Title (with link to ToR)	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group responsible	Due Date	Actual Completion Date	Status	CSEC Comments (For internal Use)	CSEC Comments (For OCSEC)	Update Required? (y/n)
84	IRRELEVANT															
83																
82	0	Spot Check Review Summer 2014	Spot Check Review of SIGINT Private Communications used or retained by CSE	No recommendations	n/a	August-14-2014	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
[redacted]																
81	1	PIF 2013	Review of CSEC's Privacy Incident File (PIF) and Minor Procedural Errors Report (MPER), 2013	I recommend that CSEC request second Party Partners to confirm de-targeting of Canadians, and indicate in the PIF whether the Second Party has confirmed that it stopped targeting the Canadian.	Process	March-01-14	Accepted	Second Parties will be sent a message that asks whether or not the Canada has been de-targeted.	DGPC	D2B/SPOC	Q2 (August 2014)	2014-08-01	completed	D2 has begun sending emails that ask Second Parties to cease targeting a Canadian.	Fulfilled: CSE updated relevant procedures to implement the process outlined in the recommendation.	n
80	1	SIGINT MAs 2013	Review of CSEC's 2013 Foreign Signals Intelligence Ministerial Authorizations	Recommendation 5: CSEC should promulate guidance regarding the treatment of [redacted] acquired as part of [redacted] collection, but which [redacted] constituted a private communication or a two-end Canadian communication.	Policy and guidance/business practices	March-01-14	Accepted	Recommendation accepted with modifications. DGPC and SIGINT to co-ordinate and identify key scenarios by Q1 2014-15 with related guidance issued by Q2.	DGPC/SIGINT	D2B/SPOC	KEY SCENARIOS Q3 2014-2015 RELATED GUIDANCE Q4 2014-2015		In Progress	2014: Initial timeline delayed - Scenarios still in development ; 2015: The recommendation related to a very specific set of circumstances that arose in the review. Responsibility for implementation will rest with SPR1.	In Progress: In FY 2014-15, priority was placed on implementing solutions to address recommendations 3 and 4, and to updating CSOI-4-3. CSE will address this recommendation and implement guidance in the coming fiscal year.	y
80	1	SIGINT MAs 2013	Review of CSEC's 2013 Foreign Signals Intelligence Ministerial Authorizations	Recommendation 1: to ensure proper accountability for sensitive activities, CSEC should promulgate detailed guidance, as soon as possible, regarding the additional approvals required for certain activiites relating to the [redacted] program and to CSEC operations [redacted]	Policies and procedures	March-01-14	Accepted	Recommendation accepted. DGPC will reissue guidance relating to the approval process for [redacted] as an annex to OPS-1-13 (Q3 FY 2014-2015). DGPC and SIGINT will develop policy guidance relating to the approval process for [redacted]	DGPC/SIGINT	D2B/SPOC	Q3 2014-2015	2015-03-01	completed	DGPC will reissue guidance relating to the approval process for [redacted] as an annex to OPS-1-13 . DGPC and SIGINT will develop policy guidance relating to the approval process for [redacted] Expected to be completed by end of Q3 FY 2014-2015 Update: OPS 1-13 was finalized in March 2015	Fulfilled: CSE promulgated OPS-1-13 in February 2015, which included an annex relating to this recommendation.	n
80	1	SIGINT MAs 2013	Review of CSEC's 2013 Foreign Signals Intelligence Ministerial Authorizations	Recommendation 2: CSEC should make available to the Minister more comprehensive information regarding the number of intercepted communications and intercepted private communications that it acquires and retains throughout an MA period, in order to enhance accountability to the Minister	Authorities	March-01-14	Accepted	DGPC, with support from SIGINT, will include more information in the 2014-2015 MA annual report, regarding the fluctuations in numbers of retained PCs throughout the reporting year.	DGPC/SIGINT	B/SPOC	2014-2045		In progress	Recommendation was partially satisfied by providing additional context in the recent MA report. B group and SIGINT continuing discussions to enhance information to be captured in future MA reports. April 2015: SPR2 and B group have had discussions and will continue to refine implementation. The status continues to be "in progress". SPR2 anticipates producing a mock-up for further discussion with B group (probably in June, as preparation for the next MA request memos [November], based on a monthly pull of the MA stats) that will inform what the year-end report could look like.	CSE has partially satisfied this recommendation by providing in the 2013-14 MA Year End Report, more comprehensive information regarding the number of SIGINT PCs retained throughout the reporting period. Technical developments will continue in order to provide the Minister (in the 2014-15 MA Year End report) with more detailed information regarding the fluctuations in numbers of retained SIGINT PCs throughout the reporting period.	y
80	1	SIGINT MAs 2013	Review of CSEC's 2013 Foreign Signals Intelligence Ministerial Authorizations	Recommenation 3: CSEC analysts should immediately annotate recognized private communications for essentiality to international affairs, defence or security, or for destruction, as required by the National Defence Act.	Policy and guidance	March-01-14	Accepted	Recommendation accepted. SIGINT will enforce the roles and responsibilities of analysts as identified in existing policy documentation and operational instructions.	SIGINT	SPOC	Q1	Summer 2014	completed	2014: This requirement has been included in the revised version of CSOI 4-3 (not yet promulgated). 2015: CSOI is in the approval process; but the intent of the recommendations have been met, analysts get a monthly reminder with a 30-day warning or they age off (SPOC to provide write-up to D3)	Fulfilled: As verified during the "spot check" reviews in summer and fall 2014, CSE implemented this recommendation. Meanwhile, a revised version of CSOI-4-3 has also been drafted. And will promulgated upon approval.	n
80	1	SIGINT MAs 2013	Review of CSEC's 2013 Foreign Signals Intelligence Ministerial Authorizations	Recommendation 4: CSEC analysts should regulary assess, at a minimum quarterly, whether the ongoing retention of a recognized private communication not yet used in and End Product Report is strictly necessary and remains essential to international affairs, defencr or security or whether that private communication should be deleted.	Policy and guidance	March-01-14	Accepted	Recommendation accepted. SIGINT to ensure that all analysts review their retained private communications quarterly, commencing at the end of the next quarter.	SIGINT	SPOC	Q1	2015-02-01	completed	2014: This requirement has been included in the revised version of CSOI 4-3 (not yet promulgated). Feb 2015: CSOI is in the approval process; but the intent of the recommendations have been met, analysts get a monthly reminder with a 30-day warning or they age off (SPOC to provide write-up to D3)	Fulfilled: CSE developed an automated notification system where SIGINT analysts receive notification once a month for annotated traffic that has been in the CTR for over 90 days and which has not been used in an EPR. The notification will indicate that the items listed have been automatically marked for deletion and will be deleted from the CTR in 30 days unless they are again annotated for retention. If no action is taken, the annotated traffic will be purged from the CTR in 30 days. CSE may demonstrate this notification system in the next PC Spot Check.	n
79	0	Disclosures 2013	Review of Communications Security Establishement Canada's (CSEC) disclosures of Canadian Identity Information (CII) to Government of Canada (GC) clients for calendar year 2011.	No recommendations	n/a	March-01-14	n/a						n/a			
78	1	Office of Counter Terrorism 2012	Review of the Actitivies of the Office of Counter Terrorism 2012	Recommendation 1: CSE should modify its policy OPS-1-10, Procedures for Metadata Analysis [redacted] to reflect current practices for these activities, specifically for record keeping.	Policy and guidance	October-01-12	Accepted	OPS-1-10 is currently under revision. The revised version of the policy, in addition to a new CSOI, will provide updated instruction on the OPS-1-10 process including record keeping.	SIGINT	SPOC	Q3 2014-2015		In Progress	Metadata analysis [redacted] has been halted, based on legal advice and the Chief's decision. OPS-1-10 will be cancelled and replaced by a new Operational Policy which will provide clear guidance. It is anticipated that the draft Operational Policy will be submitted for the Chief's approval by the end of FY 2014-15.	Taken over by events: CSE halted metadata analysis activities [redacted] in 2014 following the [illegible] Meanwhile, CSE is updating its policy framework to disestablish OPS-1-10 and incorporate relevant metadata analysis practices into relevant policies.	n

Review Number	Recommendation Number	Review - Short Title	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date / Date of the Email	Recommendation Accepted?	CSEC Management Response	Business Line Responsible	Owner (Organization)	Due Date	Actual Completion Date	Status	CSEC Comments on Implementation	CSEC Comments on OCSEC	Update Required? (y/n)
78	2	Office of Counter Terrorism 2012	Review of the Activities of the Office of Counter Terrorism 2012	Recommendation 2: CSE should promulgate guidance to codify its practices to address cases when an analyst identifies that a Second Party is targeting a Canadian, including notification to the Second Party to desist from such targeting and record keeping of such	Policy and guidance	October-01-12	Accepted	In coordination with SIGINT, DGPC's Privacy and Interest Protection Team (D2A) will develop and promulgate guidance regarding the procedures that analysts should follow, if they determine a Canadian is being targeted by a Second Party.	DGPC	D2A	This will be completed Q2 (August) but interim guidance will be issued to D2 staff in relation to the recommendation at that time as well.		In Progress	Guidance is in development	IRRELEVANT	y
77	0	Policy Compliance Study 2012-2013	Study of Comunications Security Establishment Canada's policy compliance monitoring framwork and activities.	No recommendations	n/a	Policy jan 2014	n/a						n/a			
76	1	Second Party Info Sharing	A Review of CSEC SIGINT Information Sharing with the Second Parties	Recommendation 1: To support the Minister of National Defence in his accountability for CSEC and as an additional measure to protect the privacy of Canadians, CSEC should record and include in its Annual Report to the Minister information about the communications CSEC acquires from its Second Party partners in the United States, United Kingdom, Australia and New Zealand, including the number of one-end in Canada Second Party-collected communications, recognized by CSEC analysts and used or retained for foreign intelligence purposes, as well as the number of this type of communication destroyed.	Authorities	July-17-13	Accepted	SIGINT has confirmed that it will be possible to record and report certain supplemental data relating to communications CSEC acquires from Second Parties, such as the number of one-end in Canada Second Party-collected communications, when recognized and annotated by CSEC analysts, that have been used or retained for foreign intelligence purposes, or marked for destruction. Thisreporting will begin with the 2013-2014 Annual Report	SIGINT	SPOC	2013-2014	2014-10-01	Completed	CSE intelligence analysts already annotate this traffic and statistical information is being captured in [redacted]. It is believed that these stats were included in this year's annual report to the Minister.	Fulfilled: The 2013-2014 Annual Report to the Minister included statistics on communications CSE acquires from its Second Party partners.	n
76	1	Second Party Info Sharing	A Review of CSEC SIGINT Information Sharing with the Second Parties	Recommendation 2: To support the Minister of National Defence in his accountability for CSEC and as a measure to protect the privacy of Canadians, it is recommended that the Minister issue, under his authority pursuant to subsection 273.62(3) of the National Defence Act, a new ministerial directive to provide general direction to CSEC on its foreign signals intelligence information sharing activities with its Second Party partners in the United States, United Kingdom, Australia and New Zealand, and to set out expectations for the protection of the privacy of Canadians in the conduct of those activities.	Authorities	July-17-13	Accepted	CSEC will support the Minister in the development of a new ministerial directive to provide general direction to CSEC on its information sharing activities with its Second Party partners, with a focus on privacy and legal obligations associated with such information sharing.CSEC will begin undertaking the necessary preparatory work that will inform the development of a proposal package for an MD that will apply to both SIGINT and IT Security, and will address the following points: • The history and value of CSEC's information sharing arrangements with Second Parties; • Canada's expectations from the Five-Eyes information sharing arrangements; • Limits on information sharing and measures to protect the privacy of Canadians; • Requirements for reporting to the Minister; • Compliance monitoring; and • Review by the CSE Commissioner. CSEC expects that an MD proposal submission will be provided to the Minister for consideration by the end of fiscal year 2014/2015.	DGPC	B Group	2014/2015		In Progress	On track for finalization of MD for Q4 2014-2015. April 2015: MD updated, risk assessment still in draft	In Progress: CSE is finalizing the risk assessment and Ministerial Directive to be submitted to the Minister of National Defence.	y
75	0	AEN additional information	CSE provided information to an AEN civil litigation. OCSEC had been privy to what had already been provided under Yakabouchi and they therefore wanted to see any of the new information provided for this civil case. OCSEC then produced a letter about the information and provided that to the Minister.	No recommendations.	n/a	June 19 2013							n/a			
74	0	SIGINT MAs 2011-2012	Review of CSEC's 2010-2011 and 2011-2012 Foreign Signals Intelligence Ministerial Authorizations	No recommendations.		March-28-13							n/a			
73	0	PIF 2012	Review of CSEC's Privacy Incident File (PIF) and Minor Procedural Errors Report (MPER), 2012	No recommendations.		March-23-13							n/a			
72	0	DCII IV 2012	Annual review of a sample of CSEC disclosures of Canadian Identity Information (CII) to Government of Canada (GC) clients, 2012	No recommendations.		March-18-13							n/a			

Review Number	Recommendation	Review - Short Title (with link to TeRi)	Review - Full Title	Review Recommendation(s)	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for Internal Use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
71	1	[redacted] Review	Review of CSEC Activities Relating to an [redacted]	Recommendation 2: In light of the findings in this review, it is recommended that CSEC ensure that its foreign intelligence analysts are knowledgeable about and follow existing policy guidance, introduced since the period under review, respecting their responsibilities for determining and documenting the assessment of the foreign status of a targeted entity and the justifications for targeting that entity.	Process	February-15-13	Accepted	CSEC will continue to ensure that analysts are knowledgeable about and follow existing policies. Since the period under review, SIGINT Programs Oversight and Compliance (SPOC) was created as a primary SIGINT point of contact for policy guidance, oversight and compliance issues. In addition: Specific targeting guidance (CSOI-4-4) was introduced in 2009 which provides clear instructions to foreign intelligence analysts: CSOI-4-4 (2.1) indicates that all selectors and methods used in the collection and acquisition of information from the global information infrastructure (GII) shall be directed at foreign entities located outside Canada and associated with GC intelligence priorities; CSOI-4-4 (2.4) indicates that all targeted selectors must be managed and validated individually on an annual basis; and CSOI-4-4 (2.8) indicates that analysts are responsible for conducting research and documenting that all conditions for targeting have been met, including the foreign assessment and documentation. A mandatory annual OPS-1 quiz, combined with the Foundational Learning Curriculum (FLC), SIGINT 101 and on-the-job training helps to ensure that all SIGINT employees are knowledgeable about policy guidance. It is also worth noting that SIGINT employees who are unsuccessful on the OPS-1 quiz are subject to remedial action, including revocation of access to SIGINT systems. In 2011 SIGINT stood up a Compliance Management Team (CMT) which provides another level of assurance to SIGINT management about the level of knowledge and compliance with policy guidance.	SIGINT	SPOC	n/a	n/a	Completed			
71	1	[redacted] Review	Review of CSEC Activities Relating to an [redacted]	Recommendation 1: It is recommended that CSEC promulgate policy guidance respecting how to clearly and consistently identify in its communications with Government of Canada [redacted] whether an identifier or selector is believed to be used by an entity, used by an associate or contact of an entity, or suspected to relate to an entity.	Policy and guidance	February-15-13	Accepted	CSEC will address this issue through a policy instrument, supported by adjustments to analyst training. It is expected that this will be completed by end of fiscal year 2013/2014.	SIGINT	SPOC	March-31-14		Completed	SPOC has included this in new training. As well, they have included it in working aids on making a proper foreign assesement. SPI 1-14		
70	IRRELEVANT															
69	IRRELEVANT															
69																
[redacted]																
68	0	SIGINT MAs 2009-10	Review of CSEC's 2009-2010 foreign Intellilgence Ministerial Authorizations	No formal recommendations. Eleven related findings. (noted in the "Findings" worksheet).		March-30-12		None					N/A			N
67	0	N/A	update on an ongoing review of CSEC's foreign signals intelligence sharing [redacted]	No recommendations. This "report" was created by OCSEC to include in their annual report that they continue to work on the second party review report. For All recommendations outlined in that report please see above.									n/a			
66	0	PIF 2011	A review of privacy incidents recorded by Communications Security Establishment Canada (CSEC) in its privacy incidents file (PIF) in 2011.	No formal recommendations. The Commissioner expressed interest in three follow-on activities by CSEC: 1) CSEC issuing guidance to address a policy gap relating to CSEC analytical exchanges of CII with Second Party Partners; 2) for ITS Security, CSEC issuing guidance to its operations centre for receiving sensitive information, and 3) related to (2), CSEC will monitor the process for proactive release of such information and associated reporting. (see 934278)		March-20-12		None					N/A			N
65	0	DIAC IV (2011)	Review of Communications Security Establishement Canada's (CSEC) disclosures of Canadian Identity Information (CII) to Government of Canada (GC) clients for calendar year 2011.	No formal recommendations. The Commissioner noted that the "... usual meticulousness exhibited by the section responsible for processing disclosure requests was a little less so during the period under review... CSEC was able to provide ... clear evidence that all activities were authorized and conducted in accordance with policies and procedures.". (see 928761)		March-13-12		None					N/A			N

Review Number	Recommendation #	Review - Short Title (with link to ToR)	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for internal use)	CSEC Comments (for OCSEC)	Update Required? (Y/N)
64	0	COPCC [redacted]	A Review of CSEC's COPCC and its Activities and those SIGINT activities conducted in support of Two Major Events [redacted]	No formal recommendations. One related finding requires attention (noted in the "Findings" worksheet).		[redacted]		None					N/A			N
63	0	Retention, disposal	Review of CSEC's retention and disposal of intercepted information	No formal recommendations. Three related findings require attention (noted in the "Findings" worksheet).		December-22-11		None					N/A			N
62	0	PIF 2010	A review of privacy incidents recorded by the Communications Security Establishment Canada (CSEC) in its privacy incidents file (PIF) in 2010.	No formal recommendations. The Commissioner made three "suggestions" in his letter to DGPC (793323): 1) always include in the PIF a reference to the date that a specific action was taken by CSE relating to a privacy incident; 2) clarify entries in the "potential damages" column; 3) verify that corrective and mitigation actions are implemented, and note this in the PIF record. These were agreed to by D2 (see 804211).		July-04-11		None	n/a	n/a			N/A	No formal recommendations		Y - confirm whether suggestions have been implemented in PIF.
61	1	T&SM	A Review of CSEC SIGINT's Targeting and Selector Management Activities	Recommendation 1: CSEC should provide specific guidance for [redacted] targeting.	Policy and guidance	March-15-11	Accepted	CSE accepts this recommendation regarding the need for specific guidance in conducting [redacted] targeting activities and will incorporate this recommendation in its work plans.	SIGINT	SPOC	End FY 2011-2012		COMPLETED	**September 2011** (SPOC): Due to conflicting priorities, work on this topic has been delayed. SPOC expects to have a completed draft of specific guidance on this topic by the end of the current fiscal year (March 2012). UPDATE: New version of CSOI 4-4 was published in Dec 2013 that addresses the concerns.	**November 2012** The draft CSOI 4-4 incorporates targeting instructions for [redacted] In the meantime the SPOC Interim Guidance for Leveraging the [redacted] Program for Intelligence Reporting (updated May 2012) remains available.	
60	1	SIGINT MAs	Annual Review of CSEC's Activities Conducted Under SIGINT Ministerial Authorization	Recommendation 1: The requirement for CSEC to report to the Minister the number of recognized and destroyed private communications and solicitor/client communications should be reinserted into the ministerial authorizations	Authorities	February-25-11	Not accepted	The conditions set out in Ministerial Authorizations are based on the National Defence Act (NDA) requirements. There is no requirement in the NDA to report to the Minister the number of recognized and destroyed private communications (PCs) and solicitor/client communications. The NDA reflects elements of CSEC activities that could pose significant risk in the context of privacy and lawfulness. Recognized private communications that are destroyed obviously do not pose a risk to privacy. It is only private communications that are used or retained that CSEC reports to the Minister as these pose a potential risk to the privacy of Canadians. Moreover, CSEC already reports recognized and destroyed PCs to the Minister as part of a comprehensive annual report on the collection program governed by the Ministerial Authorization, as acknowledged by the Commissioner in his report. CSEC intends to continue to report this information.	PC	B	n/a	n/a	N/A	Commissioner accepted the Minister is "satisfied with current reporting requirements"; Commissioner went on to say "which I believe to be premised on CSEC continuing to report recognized and destroyed private communications". Note this hasn't been an MA requirement since 2007-08.		N
60	1	SIGINT MAs	Annual Review of CSEC's Activities Conducted Under SIGINT Ministerial Authorization	Recommendation 2: CSEC should report to the Minister the number of [redacted] acquired one-end Canadian communications [redacted] in a manner similar to what CSEC does for recognized private communications intercepted under the other SIGINT collection programs.	Authorities	February-25-11	Not accepted	To support the Minister with additional contextual information and given the importance the Commissioner attached to this issue [redacted] one-end Canadian emails [redacted] acquired through the [redacted] program, that are retained by CSEC on the basis that they are essential to international affairs, defence or security. Assuming no significant obstacles, CSEC will provide the available data for the current fiscal year [2012-2013] in CSEC's Annual Report to the Minister of National Defence, with full-year data to follow in future Annual Reports.	PC/SIGINT	B, SPOC	n/a		Completed		**May 2012** CSEC maintains its position that [redacted] does not constitute a private communication and therefore does not trigger a legal reporting requirement. Nonetheless, to support the Minister with additional contextual information, CSEC intends to begin compiling the number of [redacted] one-end Canadian emails [redacted], acquired through the [redacted] program, that are retained by CSEC on the basis that they are essential to international affairs, defence or security. The Chief intends to provide the available data for fiscal year 2012-2013 in CSEC's Annual Report to the Minister of National	N
60	1	SIGINT MAs	Annual Review of CSEC's Activities Conducted Under SIGINT Ministerial Authorization	Recommendation 3: Given the Importance to helping to ensure compliance and the protection of privacy, CSEC should accelerate the timeline for implementation of an improved SIGINT Active Monitoring Program.	Process	February-25-11	Accepted	CSEC considers this to be an important element in maturing the management accountability framework, as evidenced in the efforts voluntarily dedicated to an internal audit of the function. Notwithstanding the complexity and breadth of the ongoing effort, CSEC will accelerate enhancement of its Active Monitoring Program by developing a compliance validation monitoring regime, which includes a number of monitoring activities that address this recommendation. As well, the overarching operational policy will be updated accordingly.	SIGINT/PC	B, SPOC	End of Calendar year, 2011.		Completed	**September 2011** (SPOC): SPOC has developed a Compliance Validation Program in accordance with OPS-1-8; the program is currently being implemented throughout SIGINT operational areas.	A Compliance Validation Program has been developed and is being implemented throughout SIGINT operational areas.	N
59	0	DIAC III	Review of Disclosures of Canadian Identity Information to Government of Canada Clients April 1 to September 30, 2010	None. However, reference was made to the two recommendations from the DIAC II review (#55) (automation of release processes).	n/a	February-21-11	None	None	n/a		n/a	n/a	N/A	No recommendations		Y - check on status of review #55 recs.
58	0	ANST	Review of CSEC's activities under the Protection of Computer Systems and Networks of the Government of Canada Ministerial Authorizations - CSEC's Security Posture Assessment - Active Network Security Testing (ANST) Activities in 2007-2008 and 2008-2009	No official recommendations. However, two suggestions were made at the debrief: 1) JRT procedures such as the CONOP should be formalized (i.e. placed within the policy framework as Ois), and 2) isses that are recorded in compliance monitoring checklists should also include how the issues were resolved.	n/a	February-14-11	None	None	n/a		n/a		N/A	No official recommendations, however unofficial suggestions were made. These should be addressed, otherwise they will become recommendations.		Y - check on the unofficial suggestions.
57	0	Contact Chaining	A Review of CSEC's Contact Chaining Activities [redacted]	None	n/a	December-16-10	None	None			n/a	n/a	N/A	No recommendations, therefore no CSE actions		N

Review Number	Recommendation	Review - Short Title (with link to ToR)	Review - Full Title	Review Recommendation(s)	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for Internal Use)	CSEC Comments (for OCSEC)	Update Required? (Y/N)
56	0	CND MA Review (October 2010)	A Review of CSEC's Information Technology Security Activities conducted under the 2008-2009 Computer Network Defence Ministerial Authorization	None	n/a	October-18-10	None	None			n/a	n/a	N/A	No recommendations, therefore no CSEC actions		N
[redacted]																
55	1	Regular Privacy Review (DIAC II)	Regular Privacy Reviews	**Recommendation 1:** That CSEC amend Operational Policy OPS-1-1 and all associated sectional operating instructions to include specific directions or standards to ensure the consistent accounting, tracking and reporting of client request forms and the release to clients of each piece of Canadian identity information.	Policy and guidance	February-16-10	Accepted with modification	CSEC agrees with the intent of this recommendation, but will consider whether OPS-1-1 is the most appropriate policy instrument to address this issue. CSEC will provide direction to staff, in an appropriate policy instrument or working aid, to further support reporting to the Minister of National Defence on the release of Canadian identity information. The direction will be in place by 30 September 2010.	PC	D2	September-30-10	2010-10-01	Completed	**October 2010** (D2): These directions are reviewed constantly and updated as needed as staff work on requests. The Operational Policy Wiki containing these directions was in full operational use as of August 1st. This action is effectively completed.		N
55	1	Regular Privacy Review (DIAC II)	Regular Privacy Reviews	**Recommendation 2:** That CSEC give priority to the development of the automated tools necessary to enable it to accurately and consistently account for and report on the release of all Canadian identity information.	Process	February-16-10	Accepted		PC (with SIGINT Sponsorship), CIO	CIO-[redacted] D2	December-31-10		Completed	[redacted]		Y
54	1	Afghanistan MAs	Review of CSEC's activities under the *Interception Activities Conducted Jointly with the Canadian Forces in Support of Canadian Forces Operations in Afghanistan* ministerial authorizations	**Recommendation 1:** CSEC should amend OPS-1-13 [*Procedures for Canadian* [redacted] *activities*] to include, or to create a separate policy for, Afghan MA activities	Policy and guidance	January-18-10	Accepted	CSEC has amended the OPS-1-13 procedures to include more direction pertinent to activities conducted under the latest Afghanistan ministerial authorization, signed by the Minister on 3 December 2009. The revised procedures came into force on 23 December 2009, the same date as the new ministerial authorization.	PC	D2	December-23-09	2009-12-23	Completed	[redacted] D2 March 2010: This has been completed. CSEC has amended the OPS-1-13 procedures to include more direction pertinent to activities conducted under the latest Afghanistan ministerial authorization, signed by the Minister on 3 December 2009. The revised procedures came into force on 23 December 2009, the same date as the new ministerial authorization.	April 2010: CSEC has amended the OPS-1-13 procedures to include more direction pertinent to activities conducted under the latest Afghanistan ministerial authorization, signed by the Minister on 3 December 2009. The revised procedures came into force on 23 December 2009, the same date as the new ministerial authorization.	N
53	0	ITS Study	Note: Not a Review	No recommendations. Several "observations" were made - see attached observation page.	N/A	June-11-09	None Required		-	-	-	-	N/A			Y - check "observations"
52	0	NAP[redacted]A	CSEC's [redacted] Network Analysis and Prioritization and [redacted] Activities	No recommendations.	N/A	March-12-09	None Required		-	-	-	-	N/A	D3 - April 09: OCSEC withdrew recommendation #1 from the Metadata review (report#43)	OCSEC withdrew recommendation #1 from the Metadata review (report#43)	N
[redacted]																
51	IRRELEVANT															
51																
51																
51																

Review Number	Recommendation Number	Review - Short Title (with link to ToR)	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for Internal Use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
50	1	[redacted]	Review of CSEC Signals Intelligence Activities Conducted Under Ministerial Directive & Authorization [redacted]	**Recommendation 1:** To be consistent with the condition in the [redacted] Ministerial Directive, CSEC should review and update OPS-3-1 and/or the [redacted] SOP to include a definition of appropriate threat, risk and vulnerability thresholds for both the activity and personnel involved.	Policy and guidance	March-03-09	Accepted	CSEC agrees that "threat, risk and vulnerability" should be defined in order to satisfy conditions imposed by the MD governing this activity. As well, OPS-3-1 will be revised to reflect measures required to meet the MD expectation and this recommendation. Current [redacted] SoP (issued November 2011) include an annex that incorporates guidance as to how to identify risk, vulnerability and approval mechanisms.	PC	D2, SPOC	December-23-09		Completed	**Sep 2011** (D2): OPS-3-1 was revised in January 2011; however it did not include information from the SOP on risk assessment since SIGINT's definition of risk and risk assessment methodology had not been drafted at that time. D2 will coordinate with SIGINT in order to ensure that the risk assessment matrix will be reflected, as appropriate and if needed, in the next iteration of OPS-3-1. **Sep 2011** (SPOC): A risk matrix/guide is in draft form. The annual revision of the [redacted] SOPs (to be completed in December) will make wording about risk management more specific.	**Sep 2011**: OPS-3-1 was revised in January 2011, but it did not include information on risk assessment - the definition of risk and risk assessment methodology had not yet been drafted. Currently a risk matrix/guide is in draft form. Once the matrix is finalized, if necessary it will be reflected in a revised version of OPS-3-1 (the SOP itself may be sufficient). The annual revision of the [redacted] SOP (to be completed in December 2011) will make wording concerning risk	N
50	1	[redacted]	Review of CSEC Signals Intelligence Activities Conducted Under Ministerial Directive & Authorization [redacted]	**Recommendation 2:** CSEC should determine if the legal concerns and restrictions within which [redacted] techniques are considered for approval are adequately defined, documented and available to the organization.	Legal	March-03-09	Accepted	CSEC will amend the relevant policy instruments to include a process to be followed when considering [redacted] technique, and the recording of all considerations, including legal considerations, and resulting key management decision(s).	PC	D2	December-22-09		Completed	D2 - April 09: This may either be addressed in the OPS-3-1 or [redacted] SOP. Will likely be discussed concurrently with [redacted] MA renewal. October 13: OPS-3-1 has been revised for [redacted] MA renewal, and now includes a block which contains a process to be followed when considering new [redacted] techniques (para. 2.7) and a block outlining record keeping requirements (para. 2.8). [redacted] D2 March 2010: These have been completed. OPS-3-1 has been revised to respond to these recommendations. The revised OPS-3-1 has been promulgated.	April 2010: OPS-3-1 has been revised to respond to these recommendations. The revised OPS-3-1 has been promulgated.	N
50	1	[redacted]	Review of CSEC Signals Intelligence Activities Conducted Under Ministerial Directive & Authorization - [redacted]	**Recommendation 3:** CSEC should establish formal management processes related to the consideration of proposed [redacted] techniques and the recording of the consideration and resulting decision.	Process	March-03-09	Accepted	CSEC will incorporate this recommendation into a formalized process whereby management considerations and decisions will be officially recorded. The appropriate policy instruments) will be created or modified to incorporate these changes.	SIGINT	K	December-22-09		Completed	D2 - Nov 09: OPS-3-1 has been revised to respond to these recommnedations. The revised OPS-3-1 was promulgated. [redacted] D2 March 2010: These have been completed. OPS-3-1 has been revised to respond to these recommendations. The revised OPS-3-1 has been promulgated.	April 2010: OPS-3-1 has been revised to respond to these recommendations. The revised OPS-3-1 has been promulgated.	N
50	1	[redacted]	Review of CSEC Signals Intelligence Activities Conducted Under Ministerial Directive & Authorization [redacted]	**Recommendation 4:** CSEC should consider providing basic guidelines that would assist in identifying what would make a proposed [redacted] operation considered to be "particularly sensitive" and having "significant risk", thereby requiring prior Ministerial consultation [as noted in the Ministerial Directive covering this activity].	Process / Policy and guidance	March-03-09	Accepted	CSEC agrees and will incorporate definitions and guidance in the appropriate policy instruments, and will provide the documents to all personnel associated with this activity.	PC	D2/SPOC	December-22-09		Completed	D2 - April 09: This may either be addressed in the OPS-3-1 o[redacted] SOP. Will likely be discussed concurrently with [redacted] MA renewal. October 13: There was not enough time for this to be done in the revised OPS-1-3 for the current MA renewal request. Operational Policy is dependant on input from [redacted] Group and the guidelines they develop in their SOP; these guidelines will be reflected in the next rev ision of OPS-1-3 presently scheduled for October 2010. [redacted] D2 March 2010: A threat, risk and vulnerability matrix will be developed by the [redacted] team and put into their SOP. D2 is not responsible for this so D2 should no longer be the contact for updates on the status of this matrix.	April 2010: [redacted] has revised its SOPs to include a section on risk assessment, including components specific to threat, risk and vulnerability.	N
49	1	[redacted]	CSEC's Foreign Intelligence Activities Conducted under the [redacted] Ministerial Authorizations	**Recommendation 1:** That CSEC explain any "serious issues" in its [redacted] Ministerial Authorization (MA) accountability reports to the Minister, and, where there is no such issue, that it insert an explicit statement to this effect.	MA	January-13-09	Accepted	CSEC has already taken measures to have this recommendation incorporated into future Ministerial Authorizations, and into MA accountability reporting mechanisms from across the organization.	PC	B	-	-	Completed	B - April 09: In his report to the MND on 2008 SIGINT activities under MA, the CCSEC stated in his cover letter that no serious issues arose under any of the MAs, and will next year incorporate a separate statement on "serious issues identified or not identified" for each MA in the attached reporting annex. The Chief's letter to the MND was signed and forwarded to MND on April 24.	The Chief plans to state, in the covering letter accompanying his report to the MND on 2008 SIGINT activities under MA, that no serious issues arose under any of the MAs, and will next year incorporate a separate statement on "serious issues identified or not identified" for each MA in	n
48	0	DIAC	Disclosure of information about Canadians to Government of Canada clients	No recommendations.	N/A	November-13-08	None Required	-	-	-	-	-	N/A	-	-	N
47	1	[redacted] MA	CSEC's Activities Conducted Under the [redacted] Ministerial Authorizations	**Recommendation 1:** That CSEC adopt and publish, as soon as practicable, written guidance respecting the process [redacted] analysts are to follow when deciding whether to approve or reject a selector.	Policy and guidance	June-11-08	Accepted	CSEC has already drafted operational instructions to staff which document [redacted] roles, responsibilities, and processes related to selector management and validation. The operational instructions also document the oversight and management monitoring requirements for these activities. The operational instructions will be promulgated by the end of December 2008.	SIGINT	SPOC	December-31-08	0000-00-00	Completed	SPOC - April 09: On 18 September 2008, CSEC promulgated Canadian SIGINT Operation Instruction (CSOI) 3-7, [redacted] *Authorities* , which addresses the authorities and responsibilities of [redacted] analysts for selector validation. CSOI-4-4, *Targeting and Selector Management Using* [redacted] *National SIGINT Systems for Intelligence Reporting Purposes* , also provides targeting validation guidance.	On 18 September 2008, CSEC promulgated Canadian SIGINT Operation Instruction (CSOI) 3-7 [redacted] Authorities, which addresses the authorities and responsibilities of [redacted] analysts for selector validation. CSOI-4-4, Targeting and Selector Management Using [redacted] National SIGINT Systems for Intelligence Reporting Purposes, also provides targeting validation guidance.	n
47	1	[redacted] MA	CSEC's Activities Conducted Under the [redacted] Ministerial Authorizations	**Recommendation 2:** That CSEC's policies be amended to clarify that analysts must annotate for deletion all copies of a private communication found to have no FI value in all of CSEC's systems.	Policy and guidance	June-11-08	Accepted	The requirement to annotate for deletion in more than one repository will be eliminated once CSEC has transitioned to the Common Traffic Repository (CTR) by the end of December 2008. Once this transition is complete and the CTR has been fully implemented, all traffic will be held in a single data repository. In the interim and in response to an internal audit conducted prior to this review, SIGINT intelligence analysts have been directed to annotate for deletion any identical pieces of traffic from all databases.	SIGINT	[redacted]	December-31-08	0000-00-00	Completed	SPOC - April 09:Analysts were advised of their responsibilities regarding annotations. The Common Traffic Repository has been implemented, through a phased approach. As a result of the move to CTR, analysts are only required to annotate traffic in a single database. For that traffic which is not yet part of the CTR (i.e., [redacted] fax traffic), a synchronization function has been implemented so that analysts are not required to annotate in multiple databases.	Analysts were advised of their responsibilities regarding annotations. The Common Traffic Repository has been implemented, through a phased approach. As a result of the move to CTR, analysts are only required to annotate traffic in a single database. For that traffic which is not yet part of the CTR (i.e., [redacted] fax traffic), a synchronization function has been implemented so that analysts are not required to annotate in multiple databases.	n
46	1	P&T	Report to the CSE Commissioner on Protecting Privacy: Review on CSEC's Acquisition and Implementation of Technology per Subsection 273.64 (2) of the National Defence Act	**Recommendation 1:** That CSEC re-evaluate how it describes the [redacted] activities in its request for a Ministerial Authorization (MA) so as to clearly identify which activity the Minister of National Defence is authorizing when signing a [redacted] MA.	Authorities	June-11-08	Accepted	CSEC will revise how it describes the [redacted] activities in its request for an MA, as follows: The Request Letter will more clearly state that CSEC is authorized to engage in [redacted] activities under paragraph 273.64(1)(a) of the National Defence Act. Similarly, it will indicate that, in light of the inherent risk that private communications may be intercepted as a result of foreign intelligence collection activities, the Minister is authorizing the interception of any private communications that may occur while CSEC is engaged in [redacted] activities. Lastly, the Request Letter will more clearly identify those aspects of the [redacted] activities that are subject to conditions imposed by other legal instruments, such as the Ministerial Directive on the Collection and Use of Metadata.	PC	B	-	0000-00-00	Completed	B - April 09: The most recently signed [redacted] MA has fully incorporated all recommended changes.	The most recently signed [redacted] MA has fully incorporated all recommended changes.	n

A-2017-00017--03983

Review Number	Recommendation #	Review – Short Title (with link to ToR)	Review – Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation (Non-) Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for internal use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
45	1	[redacted] MD & MA	A Review of CSE Intelligence Activities Conducted Under Ministerial Directive & Authorization – [redacted]	**Recommendation 1:** Based upon the information provided and upon findings in this review, CSEC should examine its business practices to address a systemic problem of not using opportunities to collect and record evidence of lawful conduct and compliance to imposed conditions.	Process	March-28-08	Accepted	CSEC is examining its current practices as recommended. Additional measures will be implemented, as warranted. CSEC is continuing to improve its information management regime, and is implementing a significant program that will be available to all of the organization by October 2008. CSEC is confident that its new electronic information management system, along with training and awareness programs, will result in measured improvements.	PC	D & CIO & SIGINT	March-31-09	0000-00-00	Completed	ExCom determined that the following units would lead the specified elements of the response: CIO-[redacted] for CERRID deployment and CERRID training (by 31 October 2008); D Group for awareness program (initiated by 31 October 2008 with full rollout by end of fiscal (March 31, 2009)); SPR for re-examination and improvement of present practices (by 31 December 2008). MD - April 09: This recommendation has 3 components: 1-the CERRID deployment and CERRID training is completed. The IT Solution and base training are completed. 2-A broader awareness program has been initiated. A presentation to all CSEC managers is planned for the spring. 3-CSEC intends to re-examine its current practices over the coming months.	October 2009 - A presentation to all CSEC senior and middle managers regarding legal and policy compliance has been completed, and a version of it is now given to all new employees.	N
[redacted]																
44	1	Support to CSIS	Report to the CSE Commissioner on CSE Support to CSIS, Phase 1: Mandate (a)	**Recommendation 1:** CSE should consider re-examining CSIS RFIs to ensure all information required under OPS-4-2 is contained in the RFI, including the written assurance that the information was acquired lawfully and in accordance with an investigation or warrant under Section 12 of the *CSIS Act*, and linked to a Government of Canada Requirement.	Process	January-16-08	Accepted	CSEC agrees with the principle of this recommendation and over the course of the two and a half years of this review, CSEC has amended its policies and procedures to address the issues raised. Those changes have been implemented.	SIGINT	SPOC	-	-	Completed	CSEC has amended its policies and procedures to address the issues raised. Those changes have been implemented.		N
44	1	Support to CSIS	Report to the CSE Commissioner on CSE Support to CSIS, Phase 1: Mandate (a)	**Recommendation 2:** In accordance with Recommendation #1 above, as well as with Recommendation #2 from the RCMP Phase II review, CSE should re-examine its interpretation and application of mandates (a) and (c) and ensure that all decisions and resulting activities are based upon criteria that have been consistently applied and are statutorily defensible.	Legal	January-16-08	Accepted	CSEC disagrees with the principle of this recommendation and the interpretation of parts (a) and (c) of CSEC's mandate has been the subject of ongoing discussions with OCSEC. OCSEC has forwarded a discussion paper on this topic to CSEC to which a response has been provided. Further discussions are planned with OCSEC in May to address different interpretations.	PC	D	-	0000-00-00	Completed	CSEC proposed a number of scenarios for discussion around the appropriate part of the mandate to respond. A meeting was held between CSEC and OCSEC on September 8, 2008 to review the scenarios in order to ensure a common understanding of the issues, and explain how CSEC would respond under each scenario and provide the basis for that determination. CSEC subsequently provided to OCSEC on September 26 a list of CSEC current practices that have been implemented following the CSIS and RCMP reviews.		N
44	1	Support to CSIS	Report to the CSE Commissioner on CSE Support to CSIS, Phase 1: Mandate (a)	**Recommendation 3:** CSE should review the Memorandum of Understanding between CSE and CSIS dated 1 November, 1990, relating to information/intelligence exchange and operational support (Section 12 activities), to ensure it reflects current practices and agreements.	Process / Relationships	January-16-08	Accepted	CSEC agrees to work with CSIS in order to update the MoU, aiming for completion by the end of 2008.	PC	B	December-31-08	0000-00-00	Completed	**Sep 2011** (B): Completion of the CSE-CSIS General Framework MoU is imminent, at which time CSE will turn its attention to revising the s.12 sub-MoU. April 2012 (B): the CSE-CSIS General Framework MoU was signed in December 2011. Revisions to the s.12 sub-MoU are underway.	Sep 2011: the CSE-CSIS General Framework MoU is nearing completion, following which the s.12 sub-MoU will be revised.	Y
43	1	Metadata	Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005	**Recommendation 1:** CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized by intelligence analysts be accounted for.	Authorities	January-09-08	Not Accepted	CSEC believes this recommendation may be based on information that may have been taken out of context during the review. According to CSEC operational policy , the only instances where persons other than intelligence analysts may incidentally come across private communications is during an [redacted] analysis activity, used periodically to analyse the intelligence value [redacted] or to examine [redacted] As a part of this activity—under exceptional circumstances—an [redacted] These difficulties may occur for any number of reasons, such as an [redacted] CSEC operational policy dictates that any content observed during these activities may not be used for foreign intelligence purposes and is not therefore retained. Legally, there is no requirement under the SIGINT Ministerial Authorizations, the Ministerial Directive nor the National Defence Act to have anyone other than an intelligence analyst account for private communications. CSEC's current position and practice of accounting is consistent with what is required by the Minister for accountability purposes.	-	-	-	-	N/A	D3 - April 09: Recommendation withdrawn by OCSEC in report #52 (NAP[redacted]A).	Recommendation withdrawn by OCSEC in report #52 (NAP[redacted]A).	N
43	1	Metadata	Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005	**Recommendation 2:** CSE should re-examine and re-assess the legislative authority used to conduct its contact chaining activities [redacted]	Legal	January-09-08	Accepted	This matter has been the subject of ongoing discussions with OCSEC regarding parts (a) and (c) of its mandate. OCSEC has forwarded a discussion paper on this topic to CSEC to which a response has been provided. However, CSEC remains of the view that the Department of Justice interpretation is the right one. CSEC will continue working with OCSEC to address the different interpretations with a completion date of May 2008. CSEC is also working with its legal counsel to re-examine and re-assess the management direction regarding these [illegible] Policy is being revised to clarify approval authorities for these activities and will be completed by July 2008. In addition, practices have been modified to better document the case-by-case rationales regarding the appropriateness of part (a) of the mandate for these activities.	PC	D	July-31-08	July-31-08	Completed	On 10 September 2008, the Chief, CSEC signed off OPS-1-10 (Procedures for Metadata Analysis [redacted] [Update D301; Sept 08] For information about parts (a) and (c) of the mandate, and the discussions scheduled for May 2008, please see CSEC comments in review #44, recommendation #2.	-	N

A-2017-00017--03984

Review Number	Recommendation	Review Short Title (with link to TdR)	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for Internal Use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
42	1	OCT	Review of the Activities of CSE's Office of Counterterrorism (OCT) from 1 April to 31 July 2005	**Recommendation 1:** That CSE incorporate into a computerized records management system a mechanism that will, among other benefits, ensure that the Release Form for Security Line Reports is duly filled out and signed off.	Process	October-16-07	Accepted	CSE will incorporate the Release Form for Security Line Reports into a computerized records management system by mid-2008. In the interim, SIGINT will establish a standardized (hardcopy) filing system for the Release Form for Security Line Reports. Additionally, in accordance with the provisions of OPS-1-8 (Management Monitoring), SIGINT management will initiate periodic reviews of report filing, retention and sign-offs.	SIGINT	DGI	June-30-08	June-30-08	Completed	The electronic system is [redacted] The material examined at the time of the review included some reporting that was not authored in [redacted] This issue has been resolved -- all security line reporting is now authored in [redacted] as per standard reporting procedures, and therefore has the appropriate sign-off sheets associated with the hard copy records. An interim standardized hardcopy filing system was introduced in DGI. There has since been an internal DGI review, and some adjustments may be made to the system.	-	N
42	1	OCT	Review of the Activities of CSE's Office of Counterterrorism (OCT) from 1 April to 31 July 2005	**Recommendation 2:** That CSE consider establishing a more refined tracking system that will provide a snapshot of how effective CSE SIGINT efforts are in addressing GoC intelligence priorities.	Process	October-16-07	Accepted	CSE has developed a robust system designed to provide relevant foreign intelligence to Government of Canada (GC) clients based on their individual stated intelligence priorities and linked to overall GC intelligence priorities. The system is further designed to facilitate the collection of client feedback on SIGINT reporting. This feedback provides CSE with the most accurate measures possible of how effective CSE SIGINT efforts are in addressing overall GC intelligence priorities	SIGINT	-	June-30-08	June-30-08	Completed	-	-	N
41	1	ITS [redacted] MA	Review of the CSE ITS Activities Conducted Under Ministerial Authorization at [redacted] from Nov 2004 to Nov 2005	**Recommendation 1:** Consistent with previous reviews, we recommend that CSE develop policy requiring that a CSE corporate file be established for each ITS activity undertaken under the authority of the Minister of National Defence.	Policy and guidance	March-20-07	Accepted	Internal policy direction requiring the establishment of corporate records specific to operations under MA (ORG-2-2) was signed-off and officially promulgated in April 2007. Creation of a complete corporate file for each ITS MA exercise is now required.	ITS	-	-	-	Completed	-	-	N
41	1	ITS [redacted] MA	Review of the CSE ITS Activities Conducted Under Ministerial Authorization at [redacted] from Nov 2004 to Nov 2005	**Recommendation 2:** Consistent with previous reviews, we recommend that CSE determine what constitutes the key information that should be retained on file related to the execution of an ITS MA.	Policy and guidance	March-20-07	Accepted	The basic list of required contents for MA files has already been identified and articulated in ORG-2-2. This policy, along with other relevant ones currently in revision (OPS-1-9 and OPS-1-14), will be reviewed to ensure that the execution phase of operations is adequately covered in the contents of each MA file.	PC	D	-	-	Completed	The effective date of OPS-1, OPS-1-8 and OPS-1-14 is 18 March, 2008.	-	N
[redacted]																
40	1	CRO Review	Review of the Role of CSE's CROs and D2 in the Release of Canadian Identities	**Recommendation 1:** If the Memorandum of Understanding (MOU) between DFAIT and CSE cannot be located, it is recommended that a replacement MOU be prepared	Process / Relationships	March-30-07	Accepted	CSE has conducted an extensive search for this MOU, as has DFAIT. Regrettably, neither organization has been able to produce a copy of the agreement. Accordingly, CSE has already commenced the internal development of a new MOU with DFAIT. The MOU was completed and signed on 24 November 2011.	SIGINT	A	March-01-08	0000-00-00	Completed	B - April 09: CSEC and DFAIT signed an updated Framework MoU in 2008. The General Framework MOU with DFAIT is the overarching document that sets out where/how the two organizations will cooperate. [redacted] The general framework MoU does not really touch on the role of CROs -- [redacted] **March 2011** (B): CSE and DFAIT will continue to work on establishing an MoU regarding CRO service at DFAIT. (In a phone conversation with [redacted] he confirmed there is an MoU circulating for comments, concerning CROs at DFAIT **Sep 2011** (B): nothing to add, except SIGINT has finalized a draft concerning CROs, and it is now with DFAIT.	**Sep 2011**: Work on a CSE-DFAIT MoU regarding CRO service at DFAIT continues; a draft is under review and should be signed before the end of the calendar year.	Y
40	1	CRO Review	Review of the Role of CSE's CROs and D2 in the Release of Canadian Identities	**Recommendation 2:** That, where practical, more comprehensive and frequent training for clients be conducted, referring to the model of what is done for CSIS and PCO analysts.	Process	March-30-07	Accepted	The recommendation refers to the D2-sponsored half-day training program currently established for CSIS and PCO clients. This half-day training, or a longer session if required, will be offered to DFAIT and other Government of Canada (GC) [redacted] clients, where appropriate and feasible.	PC	D	-	-	Completed	-	-	N
40	1	CRO Review	Review of the Role of CSE's CROs and D2 in the Release of Canadian Identities	**Recommendation 3:** That, where feasible for other clients, CSE follow the model it has established for direct, secure electronic communication between CSIS analysts and CSE/D2 to make requests.	Process	March-30-07	Accepted	In expanding CSE's [redacted] (self-serve) program there are a number of considerations related to technology, finances, and client preference. Whereas there have been some relatively recent additions, such as CBSA, RCMP/SIHU (Special Information Handling Unit), and Public Safety Canada's Emergency Management and National Security Branch, in other cases, such as DFAIT, departments or sub-elements of departments opt instead for CRO service in order to maintain a high level of personal service to their middle- and higher-level managers. Should DFAIT or other GC clients at any time request expansion of [redacted] service among their analyst communities, CSE will incorporate considerations for requesting identity information. This, in combination with the training discussed above, should serve to improve the overall level of consistency in identity requests.	SIGINT	A	-	-	Completed	-	-	N

Review Number	Recommendation	Review - Short Title (with link to TOR)	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for internal use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
40	1	CRO Review	Review of the Role of CSE's CROs and D2 in the Release of Canadian Identities	**Recommendation 4:** That CSE re-examine its processes with respect to the release of the same ident to individual clients within the same department or agency, with the objectives of i) ensuring consistency of application; and ii) of accounting for each release, including multiple releases of the same ident, within a client department or agency and thus ensuring more accurate statistics.	Process	March-30-07	Accepted with modifications	With respect to the first aspect (i) of the recommendation, CSE will re-examine its existing procedures, to ensure consistency of application when receiving multiple requests from a given organization for Canadian identity information suppressed from a given report, and CSE/D2 will review, process and file each request individually. Satisfying the second aspect (ii) of the recommendation would require imposing additional process on SIGINT clients requiring them to return to CSE for permission to share identity information with their indoctrinated departmental colleagues. We assess that this would be cumbersome from the client's perspective, and unenforceable from CSE's, and prefer instead to rely upon each department's Privacy Act obligations to ensure proper handling of the information. That said, CSE will address the statistical consistency issue by tabulating, for metrics purposes, only the release of identity information to a given organization, and not to individuals within the organization.	PC	D	-	-	Completed	At the request of the CSIS Liaison Officer, CSIS is the only department that can make multiple requests for the same identity. As for ii) accounting for each release, including multiple releases of the same identification, within a client department or agency and thus ensuring more accurate statistics: We save all identity releases in a central folder, so they're all accounted for. That said, CSEC will address the statistical consistency issue by tabulating, for metrics purposes, only the release of identity information to a given organization, and not to individuals within the organization.	-	N
40	1	CRO Review	Review of the Role of CSE's CROs and D2 in the Release of Canadian Identities	**Recommendation 5:** That CSE examine the disclosure of idents under the Privacy Act with a view to amending the Request for Release of Suppressed Information form to include the section of the Privacy Act that is the appropriate authority.	Process	March-30-07	Accepted	CSE will undertake to re-examine the disclosure of idents under the Privacy Act. Solicitor-Client Solicitor-Cl stemming from a previous OCSEC review	PC	D	March-01-08	March-01-08	Completed	The form has been amended.	-	N
39	0	[redacted] MD & MA	A Review of CSE's SIGINT Activities Conducted Under [redacted] Ministerial Directive and Ministerial Authorizations - Phase I	No recommendations.	N/A	February-20-07	None Required	-	-	-	-	-	N/A	DGPC COMMENT : The preliminary research phase was aimed at delineating the authority and policy structures as well as mechanisms and processes in place to conduct the program. This phase has also allowed the Commissioner's staff to identify the components and aspects to be examined in the second phase, which will concentrate on program implementation and execution.		N
38	1	ITS [redacted] MA	A Review of CSE's Information Technology Security Activities Conducted Under the [redacted] Ministerial Authorization	**Recommendation 1:** We recommend that CSE establish a policy that requires the [redacted] during the execution of an SPA exercise.	Policy and guidance	December-18-06	Accepted	CSE existing practices already include the [redacted] during the execution of a Security Posture Assessment (SPA) exercise. However, CSE recognizes that these practices are not required by the existing formal policy direction on conducting SPA activities (OPS 1-9). CSE is currently amending the policy.	PC	D	March-31-07	March-31-07	Completed	The effective date of OPS-1-9 Procedures for Security Posture Assessments (SPA) is 18 December 2007and includes a requirement for [redacted] and a record to be kept thereof. The effective date of OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, OPS-1-8 [redacted] of Operations to Ensure the Legal Compliance and the Protection of the Privacy of Canadians and OPS-1-14 Procedures for Computer Network Defence (CND) Activities is 18 March, 2008	-	N
38	1	ITS [redacted] MA	A Review of CSE's Information Technology Security Activities Conducted Under the [redacted] Ministerial Authorization	**Recommendation 2:** We recommend that CSE require that a record of the active monitoring of staff activities and an assessment of the conduct of staff during the execution of a SPA exercise be placed on file.	Policy and guidance	December-18-06	Accepted	The relevant operational policy direction (OPS1-9 and ORG 2-2) will be updated to include a requirement to produce a record of the [redacted] and to place the record on the corporate file.	PC	D	March-31-07	March-31-07	Completed	The effective date of OPS-1-9 Procedures for Security Posture Assessments (SPA) is 18 December 2007and includes a requirement for [redacted] and a record to be kept thereof. The effective date of OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, OPS-1-8 [redacted] of Operations to Ensure the Legal Compliance and the Protection of the Privacy of Canadians and OPS-1-14 Procedures for Computer Network Defence (CND) Activities is 18 March, 2008. The effective date of ORG-2-2: Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization is 13 April 2007.	-	N
38	1	ITS [redacted] MA	A Review of CSE's Information Technology Security Activities Conducted Under the [redacted] Ministerial Authorization	**Recommendation 3:** We recommend that CSE provide direction and establish a means to effectively assess the appropriateness of information appended to final reports and to determine the essentiality of retaining this appended information as part of the CSE corporate record.	Process / Legal	December-18-06	Accepted	While CSE accepts the proposed actions since it represents good business practice, CSE does not agree that this is a lawfulness issue as suggested. CSE will continue discussions with the Commissioner's staff on this matter to further clarify CSE's position while seeking a resolution.	PC	D	October-31-07	October-31-07	Completed	ITS: Interim assessment criteria to be developed and implemented by the end of February 2007; (policy to be formally revised by 31 March 2007). John Bruce, CSE Legal Services (DLS) provided [22 Jan 07] a S Solicitor-Clien **((Review 29 Feb 08))**	-	N
38	1	ITS [redacted] MA	A Review of CSE's Information Technology Security Activities Conducted Under the [redacted] Ministerial Authorization	**Recommendation 4:** Consistent with previous reviews, we recommend that CSE develop policy requiring that a CSE corporate file be established for each ITS activity undertaken under the authority of the Minister of National Defence.	Policy and guidance	December-18-06	Accepted	Internal policy direction requiring the establishment of corporate records specific to operations under MA (ORG 2-2) is in the final stages of review prior to management sign-off and official promulgation. Creation of a corporate file for each IT Security MA is, however, already in practice.	PC	D	March-31-07	March-31-07	Completed	The effective date of ORG-2-2: *Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization* is 13 April 2007.	-	N
38	1	ITS [redacted] MA	A Review of CSE's Information Technology Security Activities Conducted Under the [redacted] Ministerial Authorization	**Recommendation 5:** Consistent with previous reviews, we recommend that CSE determine what constitutes the key information that should be retained on file related to the execution of an ITS MA.	Process	December-18-06	Accepted	The basic list of required contents for MA files has already been identified and articulated in ORG 2-2. This policy, along with other relevant ones currently in revision (OPS 1-9 and OPS 1-14), will be reviewed to ensure that documentation relating to the execution phase of operations is adequately covered in the contents of each MA file.	PC	D	February-23-07	February-23-07	Completed	-	-	N
37	1	Support to RCMP - mandate a	Report to the CSE Commissioner on CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) Phase II: CSE Mandate (a)	**Recommendation 1:** CSE should take immediate steps to implement a *hard-copy* records management system, pending the development and implementation of a corporate *electronic* information and records management system. With both systems, particular attention should be paid to managing those records that are important to safeguarding the privacy of Canadians.	Process	June-16-06	Accepted	This recommendation has already been implemented. A practice of hard-copy file retention for operations, as well as a system for tracking requests, are now in place within SIGINT. Internal policy direction requiring the maintenance of hard-copy records specific to operations under MA (ORG-2-2) is in circulation for management sign-off. Implementation of the enterprise-wide electronic information management system is currently in progress, and is slated for completion in FY 07/08.	CIO	-	-	-	Completed	-	-	N

Review Number	Recommendation Letter	Review - Short Title (with link to ToR)	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for Internal Use)	CSEC Comments (for OCSEC)	Update Required? (Y/N)
37	1	Support to RCMP - mandate a	Report to the CSE Commissioner on CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) Phase II: CSE Mandate (a)	**Recommendation 2:** We believe that CSE must re-examine its interpretation and application of mandates (a) and (c) and ensure that all decisions and resulting activities are based upon criteria that have been consistently applied and are statutorily defensible.	Legal / Policy and guidance	June-16-06	Accepted	CSE operations, legal, and policy staffs conferred through the summer of 2006, which included a full-day workshop on this and related issues; the results will be validated during the fall. The aim is to formalize via the new policy package on CSE support to federal law enforcement and security agencies (OPS-4-1) slated for release in the context of the CSE-RCMP MOU revision. In the meantime any requests for specific 'reactive' intelligence support of the type referred to in the review recommendation will be dealt with on an ad hoc basis in consultation with legal staff.	SIGINT	DGI (SPOC tasked D2 to respond - Oct 2010)	-	0000-00-00	Completed	**March (and Sep) 2011** (D2): A final draft of OPS-4-1 was submitted to D HQ in February 2011. Note: a revision of OPS-4-1 was originally recommended in 2005, and re-recommended in 2006. Note: this is 6 years overdue. The is now (Oct 2011) a top priority for DGPC, with Dir D, D2, B group, and DLS fully engaged in order to update the draft for final approval.	Sep 2011: A draft of OPS-4-1 was submitted for review in February 2011. It is currently a top priority for DGPC, with stakeholders fully engaged in order to update the draft for final approval. **November 2012** The updated OPS 4-1 policy is in the final stages of review for sign off. OPS 4-1 was signed off with an effective date of 1 January 2013.	Y
37	1	Support to RCMP - mandate a	Report to the CSE Commissioner on CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) Phase II: CSE Mandate (a)	**Recommendation 3:** CSE should re-examine the authorities governing collection, use and disclosure of personal information as established in, and governed by, the *National Defence Act* and *Privacy Act*, and in particular, re-examine its interpretation and application of those authorities that govern the disclosure of Canadian personal information to the RCMP and other clients.	Legal	June-16-06	Accepted	CSE, through its legal advisors, is re-examining the authorities currently used. Advice is anticipated by early November 2006, after which any necessary amendments to the internal policy guidance (OPS-1-1) will be identified and developed.	PC	D	April-01-07	April-01-07	Completed	DLS Statement : CSE would like to note that the review has been concluded, following consultations between CSE's Directorate of Legal Services and Justice colleagues from the Information Law and Privacy Section[Mid-Sept 07]. As a result of this work, the CSE release forms will be slightly modified to indicate the authority for the release of personal information (identities).	-	N
37	1	Support to RCMP - mandate a	Report to the CSE Commissioner on CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) Phase II: CSE Mandate (a)	**Recommendation 4:** CSE should establish agreements with client agencies permitting that the information (including foreign and Canadian personal information) collected by CSE when providing operational assistance under its (c) mandate be disclosed to CSE if requested by CSE or deemed appropriate by the client agency.	Process	June-16-06	Accepted	CSE and CSIS have implemented a practice by which CSIS, when providing information/material to CSE under a mandate (c) request, may under S.19 of the CSIS Act also disclose that information to CSE to allow for the extraction of foreign lead information and production of intelligence under mandate (a). In future CSE will, on an ad hoc basis, determine whether similar agreements would be worthwhile for other departments, and will engage legal and policy staffs in response to any issues that arise around the uses to which such information would be put.	SIGINT	[redacted]	December-31-06	December-31-06	Completed	-	-	N
[redacted]																
36	1	ITS MAs for SPAs and CNDs	ITS MAs for [redacted] SPAs [redacted] CND (CSE Information Technology Security Activities Conducted Under Ministerial Authorization)	**Recommendation 1A:** That CSE OPS-1-9 and OPS-1-14 dealing with ITS ("Mandate B") activities be amended and integrated to eliminate the redundancy and ambiguity that currently exists between the policies for SPA and CND activities, and to clarify the different provisions for use and retention of intercepted information in the two cases.	Policy and guidance	March-29-06	Accepted with modifications	CSE has undertaken to review and amend, as necessary, OPS-1-9 and OPS-1-14 to ensure their clarity, consistency and completeness, and to meet evolving operational requirements. However, CSE sees value in maintaining distinct procedural documents for SPAs and CNDs because of significant differences in the associated legal requirements, considerations and risks.	**PC**	D	December-31-06	December-31-06	Completed	CSE has reviewed and amended, as necessary, OPS-1-9 and OPS-1-14 to ensure their clarity, consistency and completeness, and to meet evolving operational requirements. However, CSE sees value in maintaining distinct procedural documents for SPAs and CNDs because of significant differences in the associated legal requirements, considerations and risks.	-	N
36	1	ITS MAs for SPAs and CNDs	ITS MAs for [redacted] SPAs [redacted] CND (CSE Information Technology Security Activities Conducted Under Ministerial Authorization)	**Recommendation 1B:** That direction be provided for the case where a perceived attack is detected in the course of a authorized SPA in order that a CND response can be undertaken in a timely manner. In this case policy must allow for an expedient transition from the narrow short-term conditions for use and retention of intercepted private communications under the SPA MA to the broader requirements of the ensuing CND activity.	Policy and guidance	March-29-06	Accepted	This issue is being addressed concurrently with item "A" above.	**PC**	D	December-31-06	December-31-06	Completed	The effective date of OPS-1, OPS-1-8 and OPS-1-14 is 18 March, 2008	-	N
36	1	ITS MAs for SPAs and CNDs	ITS MAs for [redacted] SPAs [redacted] CND (CSE Information Technology Security Activities Conducted Under Ministerial Authorization)	**Recommendation 2:** That policy be developed requiring that a CSE corporate file be established for each ITS activity undertaken under the authority of the Minister of National Defence. The formal file should be created at the commencement of the exercise. When "working dockets" are required to be held by exercise coordinators, they should be considered a temporary extension of the corporate file, and be amalgamated with it upon exercise termination.	Policy and guidance	March-29-06	Accepted	Policy has been developed to address this issue and is undergoing management review.	**PC**	D	July-01-06	July-01-06	Completed	-	-	**N**
36	1	ITS MAs for SPAs and CNDs	ITS MAs for [redacted] SPAs [redacted] CND (CSE Information Technology Security Activities Conducted Under Ministerial Authorization)	**Recommendation 3:** That correspondence and documents related to activities performed under ITS Ministerial authorization be considered official government records and formally managed within the CSE corporate file system.	Policy and guidance	March-29-06	Accepted	Policy has been developed to address this issue and is undergoing management review.	**PC**	D	July-01-06	July-01-06	Completed	ORG-2-2: Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization Effective Date: 13 April 2007.	-	N
36	1	ITS MAs for SPAs and CNDs	ITS MAs for [redacted] SPAs [redacted] CND (CSE Information Technology Security Activities Conducted Under Ministerial Authorization)	**Recommendation 4:** That the CND and SPA Coordinators be responsible for verifying that each member assigned to an exercise team has acknowledged awareness and understanding of the appropriate Code of Ethics, and for ensuring that record of this verification is maintained as part of the formal exercise documentation.	Process	March-29-06	Accepted	-	ITS	N	-	-	Completed	-	-	N
36	1	ITS MAs for SPAs and CNDs	ITS MAs for [redacted] SPAs [redacted] CND (CSE Information Technology Security Activities Conducted Under Ministerial Authorization)	**Recommendation 5:** That the assigned responsibility for obtaining required approvals for MOU's (sic) include the necessity to maintain a record of the original signed copies of CSE executive MOU sign-off sheets as part of the formal exercise documentation.	Policy and guidance	March-29-06	Accepted	Existing policy instruments will be amended to reflect this requirement.	**PC**	D	July-01-06	July-01-06	Completed	The effective date of OPS-1-9 Procedures for Security Posture Assessments (SPA) is 18 December 2007and includes a requirement for [redacted] of staff and a record to be kept thereof. The effective date of OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, OPS-1-8 [redacted] of Operations to Ensure the Legal Compliance and the Protection of the Privacy of Canadians and OPS-1-14 Procedures for Computer Network Defence (CND) Activities is 18 March, 2008. The effective date of ORG-2-2: *Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization* is 13 April 2007.	-	N
36	1	ITS MAs for SPAs and CNDs	ITS MAs for [redacted] SPAs [redacted] CND (CSE Information Technology Security Activities Conducted Under Ministerial Authorization)	**Recommendation 6:**That the assigned responsibility for obtaining required approvals for the MA request package include the necessity to maintain a record of these approvals as part of the formal exercise documentation.	Policy and guidance	March-29-06	Accepted	Policy has been developed to address this issue and is undergoing management review.	**PC**	D	July-01-06	July-01-06	Completed	The final DRAFT of ORG-2-2, Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization, is being circulated for signoff by DC SIGINT, DC IT Security, and CIO. The effective date of ORG-2-2: Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization is 13 April 2007.	-	N

A-2017-00017--03987

36	1	ITS MAs for SPAs and CNDs	ITS MAs for [redacted] SPAs [redacted] CND (CSE Information Technology Security Activities Conducted Under Ministerial Authorization)	**Recommendation 7:** That formal procedures be established to ensure proper and thorough documentation of the destruction of collected data at the termination of an ITS MA undertaking.	Policy and guidance	March-29-06	Accepted	The requirement for the preparation and storage of a unique, signed Certificate of Destruction at the conclusion of each ITS MA undertaking is being documented using the appropriate operational policy instruments.	PC	D	December-31-06	December-31-06	Completed	The requirement for the preparation and storage of a unique, signed Certificate of Destruction at the conclusion of each ITS MA is included in Annex 1 of ORG-2-2: *Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization* Effective Date: 13 April 2007.	-	N
35	0	[redacted] MA	Interim Report to the CSE Commissioner on CSE [redacted] Conducted Under Ministerial Authorization	No recommendations.	N/A	March-02-06	None Required	-	-	-	-	-	N/A	For 2003 and 2004 [redacted] MAs	For 2003 and 2004 [redacted] MAs	N
34	1	[redacted]	Review of the Activities of the [redacted]	**Recommendation 1:** That CSE establish a mechanism to track and verify adherence to its policy requiring that clients retain hard copy forms with Canadian identities for a maximum of two years, and that soft copies be deleted from all e-mails.	Policy and guidance	June-22-05	Accepted with modifications	OPS 1-1 will be clarified to more fully reflect the CRO and [redacted] evolutions. Placing any particular limit on the client's retention of this type of information, while arguably advantageous for privacy purposes, would not be advisable from the perspective of the operational user. Investigations and intelligence analyses frequently continue for several years, and the value of information obtained early in the process may not become apparent until much time has passed. Because the basic justification for the release of all identity information is its centrality to understanding the report concerned, its destruction amounts to the destruction of intelligence information. The guidance provided to client departments will consist of the caveat on the request/release form, which appropriately refers to their responsibilities under the ATI and Privacy Acts, augmented by security instructions that govern the handling and storage of intelligence information provided by CSE.	PC	D	September-30-06	September-30-06	Completed	In January 2006, OPS-1-1 para 7.1 was revised to allow clients at GOC departments to retain hard / soft copies of ident request forms in accordance with: classification markings, and departmental procedures related to the handling of information about Canadians. No reference is made to a specific retention period; this will now be determined by the department itself in accordance with internal departmental retention policies.	-	N
34	1	[redacted]	Review of the Activities of the [redacted]	**Recommendation 2:** That CSE institute a system to ensure that legal and policy advice, especially those relating to safeguarding the privacy of Canadians, such as release authorities , are recorded, retained and readily retrievable.	Process	June-22-05	Accepted	CSE has initiated a revision of its formal information management system and OCSEC was informed that the final delivery is scheduled for FY 2007-2008. In the interim, the Operational Policy team has enhanced its e-mail filing arrangements in order to better track policy and legal guidance on issues of operational interest.	CIO	-	March-31-08		Completed	CSE has initiated a revision of its formal information management system and OCSEC was informed that the final delivery is scheduled for October, 2008. In the interim, the Operational Policy team has enhanced its e-mail filing arrangements in order to better track policy and legal guidance on issues of operational interest. CIO Update - April 2009: CSEC has completed the implementation and training of an Electronic Document and Records Management System, which is the system of records for all corporate information produced and supports legal and policy advice. The system provides access control, retention and disposition capabilities to support the operational requirement for the maintenance of such information.	CSEC has completed the implementation and training of an Electronic Document and Records Management System, which is the system of records for all corporate information produced and supports legal and policy advice. The system provides access control, retention and disposition capabilities to support the operational requirement for the maintenance of such information.	n
34	1	[redacted]	Review of the Activities of the [redacted]	**Recommendation 3:** That, to ensure the privacy of Canadians is safeguarded: i) periodic audits be conducted on SIGINT reports to verify that proper authorities have been obtained for releasing reports based on private communications or containing information about Canadians; and ii) in accordance with OPS-1-1, 2.6, audits be conducted on activities related to the release of suppressed information (i.e. Canadian identities).	Process	June-22-05	Accepted	An audit of SIGINT reporting processes by CSE Director General, Audit, Evaluation and Ethics is currently underway. Report release authorities and releases of suppressed information will be reviewed periodically under the management monitoring regime outlined in OPS-1-8, which is being implemented now. OPS-1-1, para. 2.6 will be replaced with a review paragraph indicating that all operational procedures are subject to management monitoring, audit and to review by various government review bodies, including, but not limited to, the CSE Commissioner and the Privacy Commissioner.	DGAEE / SIGINT / PC	[redacted] / D	March-31-06	March-31-06	Completed	i) & ii) A SIGINT Legal Compliance Audit was completed in Dec 2005 and the attendant management response is being reviewed by A&E Cte. [published 12 April 2006]. Although targeting was the primary focus of that audit, it also examined report release authorities. Another audit dealing specifically with SIGINT Reporting Procedures is being presented to the A&E Cte for approval as a priority engagement in the 2006 CSE Audit Plan. These activities will also be reviewed periodically under the management monitoring regime outlined in OPS-1-8. The requisite words have been added to OPS-1-1, para.. 2.6. In addition, CSEC procedure OPS-1-1, para 2.6 has been enhanced and replaced with a review paragraph indicating that all operational procedures are subject to management monitoring, audit and to review by various government bodies, including, but not limited to, the CSE Commissioner and the Privacy Commissioner.	-	N
34	1	[redacted]	Review of the Activities of the [redacted]	**Recommendation 4:** That CSE make it a priority to establish a system to collect reliable and complete data on private communications intercepted, collected, retained, used and destroyed, and on the release of Canadian identities, to be included in an annual report on safeguarding the privacy of Canadians.	Process	June-22-05	Accepted with modifications	(Also see the "CSE Response" to "Recommendation 5" regarding the annual report on Safeguarding the Privacy of Canadians.) The release of Canadian identities is currently tracked in considerable detail, and is available to management via the Chief's dashboard. Other "information about Canadians" is tracked in terms of report sign-off procedures, however, no annotation of traffic that contains "information about Canadians" is required under CSE Ministerial Authorizations. Measures have been developed and deployed to ensure the collection of reliable and complete data on private communications retained, used and destroyed (but not intercepted or collected). These measures will be subject to periodic monitoring under OPS-1-8. It should be noted that for measurement purposes, whether CSE is acquiring information under its SIGINT mandate or protecting electronic information under its IT Security mandate, private communications are only recognized as such when viewed and so annotated by an analyst. This is consistent with the provisions in the NDA governing CSE.	SIGINT	[redacted]	-	-	Completed	-	-	N

Review Number	Recommendation Number	Review Short Title (with link to ToR)	Review Full Title	Review Recommendation	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for Internal Use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
34	1	[redacted]	Review of the Activities of the [redacted]	**Recommendation 5:** That CSE continue to produce an annual report on protecting the privacy of Canadians, as set out in its policy.	Process	June-22-05	Accepted with modifications	The necessity for an annual report on "Safeguarding the Privacy of Canadians" pre-dates CSE's enhanced authorities structure, the internal control framework that now exists, and CSE's current management information processes. This report was critical during the early-mid 1990s when these structures and vehicles did not exist, but by 2002 its readership had evaporated. More complete privacy-related information will now be available in CSE's classified annual report to the Minister and in metrics maintained internally on the Chief's dashboard. OPS-1 and OPS-1-1 will be amended accordingly, and CSE will provide OCSEC with the relevant extracts from its annual reports.	PC	B & D	June-30-06	June-30-06	Completed	-	-	N
[redacted]																
33	1	[redacted]	Review of CSE's [redacted] Program	**Recommendation 1:** [redacted]	Relationships	March-15-05	Accepted	[redacted]	SIGINT/PC	[redacted] & B	March-31-06		Completed	[redacted]	[redacted]	n
33	1	[redacted]	Review of CSE's [redacted] Program	**Recommendation 2:** [redacted]	Process	March-15-05	Not Accepted	-	-	-	-	-	N/A	[redacted]		N
33	1	[redacted]	Review of CSE's [redacted] Program	**Recommendation 3:**. That CSE formalize agreements outlining the handling, use and retention of foreign intelligence intercepts that are provided, [redacted] directly to its partners.	Process	March-15-05	Not Accepted	-	-	-	-	-	N/A	(See Review #32, Recommendation #5.)	-	N
33	1	[redacted]	Review of CSE's [redacted] Program	**Recommendation 4:** That CSE complete the implementation of a formal information management system as soon as possible to ensure corporate records can be accounted for, and easily accessed and retrieved. In the meantime, CSE should create and maintain, manually, if necessary, all [redacted] related records [redacted]	Process	March-15-05	Accepted with modifications	The recommendation has three facets: delivering the corporate IM solution; establishing an interim central [redacted] file; and searching out or creating historical records on the evolution of the program. CSE is creating a centralized information management regime that will be implemented in FY 07/08, and records generated prior to FY 07/08 will not necessarily be captured, because addressing historical gaps across the organization's holdings would be inordinately costly and time consuming. That said, a central [redacted] file within SIGINT can be established and populated with currently available records, to ensure that documentation related to [redacted] or other significant developments, are properly recorded until the corporate solution is available.	SIGINT	[redacted]	December-31-05		Completed	The recommendation has three facets: delivering the corporate IM solution; establishing an interim central [redacted] file; and searching out or creating historical records on the evolution of the program. CSE is creating a centralized information management regime that will be implemented in **October 2008**, and records generated prior to FY 07/08 will not necessarily be captured, because addressing historical gaps across the organization's holdings would be inordinately costly and time consuming. This has been completed to the extent that the documentation was retrievable / recoverable. A central file has been established in the Director SIGINT Requirements office.	CSEC's centralized management regime is fully implemented. A central [redacted] file has been established in the Director SIGINT Requirements office.	n
32	1	[redacted] MA	Review of CSE [redacted] Activities Conducted Under Ministerial Authorization	**Recommendation 1:** That CSE take action to improve the linkage between GoC foreign intelligence priorities and the tasking and targeting of [redacted] collection activities conducted under MA against specific targets, to include: (A) The creation of a formal SIGINT requirements and priorities authority, with prescribed composition and terms of reference, for the purpose of maintaining the National SIGINT Priorities List (NSPL), including Watching Briefs; (B) The initiation of an external accountability process through which the GoC S&I community is engaged in dialogue leading to regular endorsement of the NSPL (eg., quarterly meetings of the Interdepartmental Requirements Committee); and (C) The addition of a CSE targeting policy and approval procedure regarding foreign intelligence priorities. The directive should describe the process and associated responsibilities for preparing the NSPL, taking into account generic GoC and individual client inputs, the internal approval process, and the management of tasking and targeting authorizations for related collection activities.	Process	February-28-05	Accepted	SIGINT Programs [redacted] Group) has developed a process to prepare and maintain the NSPL and to map Standing Issues with associated GCRs. Formalization and external endorsement of these processes is a logical next step. An internal [redacted] Gp mgt. instruction will be developed to describe the process for developing and maintaining the NSPL, and to define the roles and responsibilities of the SIGINT requirements and priorities authority and of the external endorsement body. The management of tasking and targeting authorizations for related collection activities should continue to be addressed separately in OPS procedures specific to these activities, but with explicit linkage to the revised NSPL process.	SIGINT	[redacted]	March-31-06	March-31-06	Completed	GCRs are now mapped to NSPL standing issues; all [redacted] tasking authorities contain references to NSPL and GCR items. The NSPL Process has been approved and promulgated within SIGINT. Due to changes in the S&I community committee structure, the interdepartmental Requirements Committee no longer exists and has yet to be replaced. The NSPL CSE SIGINT Operations Instruction (CSOI) now states that key external clients and stakeholders will vet and concur on any changes to the Standing Issues list.	-	N
32	1	[redacted] MA	Review of CSE [redacted] Activities Conducted Under Ministerial Authorization	**Recommendation 2:** That in preparing future MA requests, CSE should provide more specific qualification of the GoC foreign intelligence priority which is believed to justify the interception of private communications acquired by the proposed method of collection. This can be achieved by direct reference to the current National SIGINT Priorities List item(s) which relates to the collection activities authorized.	Authorities	February-28-05	Not Accepted	Note, however, that CSE will make general reference to the approved GoC Intelligence Requirements and attach them as an annex to individual FI MA applications.	PC	B	-	-	N/A	The NSPL changes as events and client needs evolve, so reference to it would be of limited value because priorities will shift throughout the duration of an MA. Relying upon a specific item for the Minister's decisions could also have the unfortunate consequence of either restricting CSE's ability to identify and pursue unanticipated avenues of inquiry, or reducing its ability to change the relative priority of items on the NSPL.	-	N
32	1	[redacted] MA	Review of CSE [redacted] Activities Conducted Under Ministerial Authorization	**Recommendation 3:** That CSE centralize mission management responsibilities within SIGINT Programs for all foreign intelligence collection programs where Ministerial authorization for interception of private communications is required. Responsibilities should include the maintenance of a record of decisions on alternatives considered and the basis for selection in each case	Process	February-28-05	Accepted	-	SIGINT	[redacted]	October-31-05	October-31-05	Completed	This has been partially implemented - collection decisions w.r.t. to [redacted] and [redacted] are all channelled through SIGINT/AMM (now SIGINT Requirements within DGP). Discussions concerning [redacted] have been finalized. The initial set of collection authorizations for this program will be channeled through SIGINT Requirements by the end of May 2007. This means that all collection authorizations for programs conducted under a MA are reviewed within DGP.	-	N
32	1	[redacted] MA	Review of CSE [redacted] Activities Conducted Under Ministerial Authorization	**Recommendation 4:** That CSE establish formal criteria for use by analysts in assessing the essentiality of information involving private communications. This "essentiality test" should consist of written guidelines to assist analysts with decisions on whether private communications are essential to international affairs, defence, or security in a given situation.	Policy and guidance	February-28-05	Not Accepted	Notwithstanding, OPS procedures now include an essentiality test, which is also being incorporated into the overarching OPS-1 privacy policy. The essentiality test--"A private communication will be considered essential to international affairs, defence or security only if it contains information that is clearly related to the intelligence priorities of the GoC"--is now used in the FIPs, GCRs and NSPL processes.	-	-	-	-	N/A	An essentiality test that is too restrictive will erode intelligence analysts' ability to identify and pursue unanticipated avenues of inquiry.	-	N

Review Number	Recommendation	Review - Short Title (with link to ToR)	Review - Full Title	Review Recommendation	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for Internal Use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
32	1	[redacted] MA	Review of CSE [redacted] Activities Conducted Under Ministerial Authorization	**Recommendation 5:** That CSE seek agreement among the Second Party partners on mutually acceptable measures covering the use and retention of recognized private communications intercepted through collection. The purpose would be to more formally address the intended provisions of the condition of par.273.65(2) of the Act for those instances where Second Parties are involved. (An appropriate forum for this policy might be the regular Quinquepartite Reporting Policy Conference.)	Process / Relationships	February-28-05	Not Accepted	-	-	-	-	-	N/A	This recommendation was of concern for partnership reasons. Quinquepartite partners have long-standing arrangements in place for treating 2nd Party identities according to the privacy policies of the respective 2nd Party counterpart. These agreements are well articulated through our respective documented policies and procedures. NSA also has strict policies that limit access to non-minimized raw traffic. Notwithstanding, CSE will continue to ensure that mention of mutual respect for privacy concerns be stated wherever appropriate in future agreements and shared policies.	-	N
31	1	Support to RCMP - mandate a	CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) - mandate 'c'	**Recommendation 1:** CSE should update the Ministerial Directive entitled *CSE Support to Law Enforcement and National Security Agencies*, dated June 19, 2001 in light of the passage of Part V.1 of the *NDA*.	Authorities	January-07-05	Accepted	It is integral to our plan to revisit all three of the original MDs that pre-date legislation. This work was initiated during 1st quarter of FY 05/06, and the revised MDs will be ready for signature by our Minister on completion of the *Anti-Terrorism Act* review.	PC	B	Completion of ATA review	0000-00-00	Completed	**March 2011** (B): CSEC recognizes the importance of updating all authority instruments such that they are consistent with CSEC legislation. Given the delay in proceeding with anticipated amendments to CSEC legislation, the Chief, CSEC has directed that the pre-legislation MDs on Support to Lawful Access, Privacy and Accountability be updated to meet the Commissioner's observation (#44, observation 1). The MDs are being addressed in priority sequence, beginning with Support to Lawful Access as this MD was also subject to a specific Commissioner recommendation (#31, recommendation 1). CSEC has completed initial analysis of the Support to Lawful Access MD and has identified a number of potential revisions to update the MD in keeping with current CSEC legislation and to provide greater clarity on the nature of CSEC technical and operational assistance to federal law enforcement and security agencies. Similar analysis will be completed for the Privacy and Accountability MDs to identify any revisions required for consistency with legislation. This work will continue through 2011-2012 and it is anticipated that updated MDs will be submitted for ministerial signature before the end of the fiscal year. **Sep 2011**: B-group stated there is no new information. The CSE support to Federal Law Enforcement and National Security Agencies MD was signed on 21 November 2011. The accountability and Privacy MDs have been revised following PING and will be part of the 2012 signing package.	**Sep 2011**: Given the delay in proceeding with anticipated amendments to the NDA, the Chief has directed that pre-legislation MDs be revised in order of priority (starting with Support to Lawful Access). Potential revisions to the SLA MD have been identified. Work will continue through 2011-2012, with the anticipation that the MD will be submitted for Ministerial signature before the end of the current fiscal year. The CSE support to Federal Law Enforcement and National Security Agencies MD was signed on 21 November 2011.	Y
31	1	Support to RCMP - mandate a	CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) - mandate 'c'	**Recommendation 2:** CSE should update the CSE - RCMP Memorandum of Understanding of June 21, 1995.	Relationships	January-07-05	Accepted	To date, we have developed internal principles for cooperation, have clarified and confirmed the underlying mandate application issue, have reached agreement with allies on the sharing of cryptanalytic technical information, and are engaged with CSIS and RCMP in a working group aimed at mapping cooperative arrangements. The end-state depends on achieving wider interdepartmental consensus on the composition of an expanding federal law enforcement community, and on principles for intelligence support to that community.	**PC**	B & D	December-31-05		Completed	D3 E-Mail of 16 Nov 07 : CSEC intends to update the RCMP/CSEC MoU as proposed. However, CSE's ExCom has recently decided that they will have senior level engagements with members of the RCMP senior management in order to ensure that there is a common understanding of support that CSE can (and is willing to) provide to the RCMP under our legislative mandate, while weighing the risk to disclosure of sensitive information and techniques. Once these discussions have occurred, B and D Group in DGPC will engage their counterparts to work towards an update or redrafting of the existing MoU, as required. Seniors in both organizations met in February and March and plan ot meet again to identify common strategic directions and to finalize the framework for the MoU. B Email - April 09: We will be looking at updating the SLA MD, per some work that B Group already in this area a while back. D2 -Dec'09 - The RCMP/CSEC MoU was signed 23 June 2009.	October 2009 - The RCMP/CSEC MoU was signed 23 June 2009.	N
31	1	Support to RCMP - mandate a	CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) - mandate 'c'	**Recommendation 3:** CSE should amend and update its operational procedures, OPS-4-1, entitled *Procedure for CSE Support to Law Enforcement*, dated 20 November 2001.	Policy and guidance	January-07-05	Accepted	A second draft of OPS-4-1, *Procedures for CSE Assistance to Canadian Federal Law Enforcement and Security Agencies*, has been updated: the third draft is in circulation for comments with a target for completion and signatures by 31-Oct-05. Enhanced processes for tracking operations and making risk management decisions were established in SIGINT during FY 05/06.	**PC**	B & D	October-31-05		Completed	**March 2011** (D2): A final draft of OPS-4-1 was submitted to D HQ in February 2011. Note: this is six years overdue. **Sep 2011** (D2): The is now (Oct 2011) a top priority for DGPC, with Dir D, D2, B group, and DLS fully engaged in order to update the draft for final approval.	**Sep 2011:** A draft of OPS-4-1 was submitted for review in February 2011. It is currently a top priority for DGPC, with stakeholders fully engaged in order to update the draft for final approval. **November 2012** An updated OPS-4-1 policy is currently under final review by DLS in anticipation for final approval and signoff by DCSIGINT and DCITS. OPS 4-1 was signed off with an effective date of 1 January 2013	Y
31	1	Support to RCMP - mandate a	CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) - mandate 'c'	**Recommendation 4:** CSE should include formal definitions and terminologies in any new or amended supporting documents in order to ensure consistent understanding and application.	Policy and guidance	January-07-05	Accepted	Operational Policy section (D2) has developed a master lexicon that was provided to OCSEC, and which will be used in the development of all new policy instruments. The new OPS-4 policy & procedure documentation will address the specific terms mentioned in the report. A French lexicon is also under development.	**PC**	B & D	31-Sep-05		Completed	**March 2011** (D2): The revised draft of OPS-4-1 contains a "definitions" section. Note: this is six years overdue. **Sep 2011** (D2): The is now (Oct 2011) a top priority for DGPC, with Dir D, D2, B group, and DLS fully engaged in order to update the draft for final approval.	**Sep 2011:** The draft of OPS-4-1 contains a definitions section. November 2012 Both English and French lexicons were released in July 2012.	Y
31	1	Support to RCMP - mandate a	CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) - mandate 'c'	**Recommendation 5:** CSE should develop a policy that clearly articulates CSE's role in providing support to law enforcement pursuant to the organization's legislated mandate as stated in Part V.1, sub-section 273.64 (1) of the *NDA*.	Policy and guidance	January-07-05	Accepted	A second draft of OPS-4, *Policy on CSE Support to Canadian Federal Law Enforcement and Security Agencies*, has been updated: the third draft is in circulation for comments with a target for completion and signatures by 31-Oct-05.	**PC**	B & D	October-31-05		Completed	**March 2011** (D2): The revised draft of OPS-4-1 contains the required information. The draft was submitted to D HQ in February 2011. Note: this is six years overdue. **Sep 2011** (D2): The is now (Oct 2011) a top priority for DGPC, with Dir D, D2, B group, and DLS fully engaged in order to update the draft for final approval.	**Sep 2011:** The draft of OPS-4-1 contains the required information. **November 2012** An updated OPS-4-1 policy is currently under final review by DLS in anticipation for final approval and signoff by DCSIGINT and DCITS. OPS 4-1 was signed off with an effective date of 1 January 2013.	Y
31	1	Support to RCMP - mandate a	CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) - mandate 'c'	**Recommendation 6:** Pending an updating of the MD (reference Recommendation no. 1), CSE should ensure that its personnel are informed that the Ministerial Directive on CSE Support to Law Enforcement is still in force and applicable to CSE's activities in support of the RCMP.	Process	January-07-05	Accepted	An email communication was sent to SIGINT and ITS operations staffs, via their managers, in December 2004. Coverage of MDs has been included in a comprehensive Policy Awareness course that is being offered to all SIGINT analysts beginning on 9 September 05 (after which time the course will be included in the SIGINT Baseline Program).	PC	D	-	-	Completed	-	-	N
31	1	Support to RCMP - mandate a	CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) - mandate 'c'	**Recommendation 7:** CSE should clarify what activities it can conduct under each of its three legislated authorities.	Legal / Policy and guidance	January-07-05	Accepted	Clarification with respect to parts (a) and (c) of CSEC's mandate will be included in the new OPS-4 policy package (October 05). It will also be addressed in OPS-1-10, *Procedures for Metadata Analysis* [redacted] CSEC's understanding of the limits of its three legislated mandates is evolving incrementally, based on consultation with the Department of Justice, as new operational demands and circumstances come to the fore.	PC	B & D	October-31-05	2013-01-01	Completed	**March 2011** (D2): A final draft of OPS-4-1 was submitted to D HQ in February 2011. Note: this is six years overdue. **Sep 2011** (D2): The is now (Oct 2011) a top priority for DGPC, with Dir D, D2, B group, and DLS fully engaged in order to update the draft for final approval.	**Sep 2011:** A draft of OPS-4-1 was submitted for review in February 2011. It is currently a top priority for DGPC, with stakeholders fully engaged in order to update the draft for final approval. OPS-1-10 became effective as of June 25th, 2010. **November 2012** An updated OPS-4-1 policy is currently under final review by DLS in anticipation for final approval and signoff by DCSIGINT and DCITS. OPS 4-1 was signed off with an effective date of 1 January 2013.	Y

Review Number	Recommendation Number	Review - Short Form Title	Review - Full Title	Review Recommendation	Recommendation Category	Review Report Date (yyyy-mm-dd)	Recommendation Status (Accepted / Not Accepted)	CSEC Management Response	Responsible Area	Office of Primary Interest	Due Date	Revised Completion Date	Status	CSEC Comments on Implementation	CSEC Comments on OCSEC's Assessment	Action Required?
31	1	Support to RCMP - mandate a	CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) - mandate 'c'	**Recommendation 8:** CSE should develop an agreement to govern the retention / destruction of data acquired as a result of technical assistance provided to the RCMP.	Process / Policy and guidance	January-07-05	Accepted	Auditability of RCMP support requests was enhanced during the past year with establishment of the coordination function in [redacted] Group. Formal direction on retention & destruction of information generated by these activities will be covered in the new OPS-4 documentation (3rd quarter FY 05/06). Any aspects requiring RCMP agreement will be incorporated in the revised MOU (3rd quarter FY 05/06). Final resolution of this issue is also related to the larger IM plan; as briefed to OCSEC staff by the CIO on 30 November 2004, delivery of corporate IM tools for the working levels of CSE commenced toward the end of FY 05/06 and will continue through FY 07/08.	PC & CIO	B & D, CIO	December-31-05	2013-01-01	Completed	**March 2011** (D2): A final draft of OPS-4-1 was submitted to D HQ in February 2011. Note: this is six years overdue. **Sep 2011** (D2): The is now (Oct 2011) a top priority for DGPC, with Dir D, D2, B group, and DLS fully engaged in order to update the draft for final approval. D2 - CSEC-RCMP MoU was signed in June 2009. **March 2011** (CIO): LAC has reviewed Mandate C material and determined that is can be dispositioned according to RDA 2008/003 Signals Intelligence function, as of March 18th, 2011.	**Sep 2011:** A draft of OPS-4-1 was submitted for review in February 2011. It is currently a top priority for DGPC, with stakeholders fully engaged in order to update the draft for final approval. It will provide the direction to implement the June 2009 RCMP/CSE MoU. Library and Archives Canada has determined that "part c" records can be dispositioned according to RDA 2008/003 Signals Intelligence function . Note: Review 63 specifically notes this recommendation has been addressed. **November 2012** An updated OPS-4-1 policy is currently under final review by DLS in anticipation for final approval and signoff by DCSIGINT and DCITS. OPS 4-1 was signed off with an effective date of 1	Y
31	1	Support to RCMP - mandate a	CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) - mandate 'c'	**Recommendation 9:** CSE should retain legal opinions and guidance in a corporate filing, retention and retrieval system.	Process	January-07-05	Not Accepted	Central record of all legal opinions are in the CSE legal services office and are accessible by CSE staff on a need-to-know basis.	-	-	-	-	N/A	Technically this has been completed, despite not being accepted at the time	-	N
30	1	[redacted]	[redacted] Review	**Recommendation 1:** That the OCSEC undertake to examine the full process and criteria for targeting of foreign intelligence entities where interception of private communications under Ministerial authorization is involved to provide assurance that the link between the client requirement, target selection, and method of collection is sufficiently clear to satisfy the conditions for authorization.	OCSEC	June-01-04	n/a	-	-	-	-	-	N/A	To be subject of separate OCSEC review.	-	N
30	1	[redacted]	[redacted] Review	**Recommendation 2:** That, for completeness, the OCSEC undertake to review the measures established by the SIGINT Information Repository for use and retention of private communications acquired through interception by [redacted] (as well as for other collection means).	OCSEC	June-01-04	n/a	-	-	-	-	-	N/A	To be subject of separate OCSEC review.	-	N
30	1	[redacted]	[redacted] Review	**Recommendation 3:**That CSE take steps to incorporate scheduling and disposition of the unique category of records acquired through [redacted] operations, including both that represented by collection traffic and that related to details of the exploitation activity, within formal departmental records policy.	Process / Policy and guidance	June-01-04	Accepted	OPS 1-11 and OPS 3-1 promulgated March and December 2004, respectively.	PC	D	-	1905-06-26	Completed	-	-	N
29	0	[redacted] MA	CSE's Activities carried out under 2002 [redacted] Ministerial Authorization - Follow-up	No recommendations. *Note: No unlawful activity noted, however Commissioner unable to provide Minister with meaningful assurance.*	N/A	April-19-04	None Required	-	-	-	-	-	N/A	See Review # 32 (MA), Recommendation #2.	-	N
[redacted]																
28	Solicitor-Client Privilege															
28																
28																
28																

A-2017-00017--03991

Review Number	Recommendation	Review - Short Title (with link to ToR)	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for internal use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
28	1	Solicitor-Client Privilege														
28	1															
28	1															
28	1															
28	1															
28	1															
28	1															
27	0	ITS MA - [redacted] SPAs	ITS Activities pursuant to Ministerial Authorizations - [redacted] SPAs	No recommendations.	N/A	March-19-04	None Required	-	-	-	-	-	N/A	Refer to study # 24 comments.	-	N
26	0	[redacted]	[redacted]	No recommendations.	N/A	March-15-04	None Required	-	-	-	-	-	N/A	-	-	N
25	0	[redacted]	[redacted]	No recommendations. Sections 16 and 21 of the *CSIS Act* are not appropriate to conduct [redacted] operations. The Commissioner believes a more appropriate framework exists in sub-sections 273.65 (1) and (2) of Part V.1 of the *NDA* whereby, under certain conditions, the Minister may, for the sole purpose of obtaining foreign intelligence, authorize CSE in writing to intercept private communications.	N/A	November-06-03	None Required	-	-	-	-	-	N/A	-	-	N

Review Number	Recommendation	Review - Short Title (with link to TOR)	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for internal use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
24	1	ITS MA - [redacted]	ITS Activities pursuant to Ministerial Authorizations - [redacted]	**Recommendation 1.** CSE undertake to develop a more precise definition of what constitutes personal information for practical application in a penetration exercise setting.	Policy and guidance	May-20-03	Accepted	OPS-1-9, *Handling of Private Communications and Personal Information in Active Network Security Testing*, includes general definition of personal information found in *Privacy Act* and based on DoJ consultations. Changes are being made to the final draft to standardize these procedures with OPS-1-14; final signatures are expected by 31 October 05.	**PC**	D	October-31-05	October-31-05	Completed	OPS-1-9, Handling of Private Communications and Personal Information in Active Network Security Testing, includes general definition of personal information based on that found in Privacy Act based on DoJ consultations. Changes have being made to the final draft to standardize these procedures within OPS-1-14 Procedures for Computer Network Defence (CND) Activities. The effective date of OPS-1-14 is 18 March, 2008.	-	N
24	1	ITS MA - [redacted]	ITS Activities pursuant to Ministerial Authorizations - [redacted]	**Recommendation 2.** Provision be made in CSE departmental records policy for a new records classification to cover the special case of personal information acquired through authorized interception, and that a schedule for retention and disposition be prescribed similar to that for other classes of personal records.	Policy and guidance	May-20-03	Accepted	OPS-1-9, *Handling of Private Communications and Personal Information in Active Network Security Testing,* outlines use and disposal of private comms. and personal information. Note: All material collected during ANST is destroyed at the conclusion of the exercise, so there is no need for a separate records classification or a retention schedule.	ITS / PC	N / D	-	-	Completed	-	-	N
24	1	ITS MA - [redacted]	ITS Activities pursuant to Ministerial Authorizations - [redacted]	**Recommendation 3.** The Concept of Operations (CONOPS) make clear provision for clean-up responsibilities for each vulnerability exercise.	Process	May-20-03	Accepted	CONOPS procedures have been updated to cover this area.	ITS	N	-	-	Completed	-	-	N
24	1	ITS MA - [redacted]	ITS Activities pursuant to Ministerial Authorizations - [redacted]	**Recommendation 4.** Throughout each vulnerability assessment exercise the [redacted] maintain an audit trail (preferably electronic) with details on [redacted] and that this record be used to inform the party responsible for the [redacted] requiring attention.	Process	May-20-03	Accepted	Active Network Security Testing (ANST) teams log all activities in [redacted] database (db). New db being tested. Also, client will be informed of any system which could not be [redacted] as specified in MOU.	ITS	N	-	-	Completed	-	-	N
[redacted]																
23	1	Lexicon	Lexicon of CSE Definitions	**Recommendation 1.** CSE amend policies and procedures to ensure consistent use and application of definitions and key terms	Policy and guidance	March-26-03	Accepted	Using OCSEC's lexicon, CSE's Operational Policy section (D2) has standardized definitions (new policies) and is reviewing and amending existing policies as required. A French lexicon is also under development.	PC	D	-	-	Completed	See related item Review #31, recommendation #4.	-	N
22	0	[redacted] MA	CSE's Activities carried out under 2002 [redacted] Ministerial Authorization	No recommendations. *Principal observation was that MA structure did not allow Commissioner to provide Minister with meaningful assurance of lawfulness.*	N/A	November-27-02	None Required	-	-	-	-	-	N/A	See Review #32 (MA), Recommendation #2.	-	N
22	0	[redacted] MA	CSE's Activities carried out under 2002 [redacted] Ministerial Authorization	No recommendations. *Commissioner to review CSE's [redacted] MA activities under his main review mandate.*	N/A	November-27-02	None Required	See Review # 29.	-	-	-	-	N/A	-	-	N
21	IRRELEVANT															
21																
21																
21																
21																
21																
21																
21																
21																
21																
21																

A-2017-00017--03992

A-2017-00017--03993

Review Number	Recommendation	Review - Short Title (with link to ToR)	Review - Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for internal Use)	CSEC Comments (for OCSEC)	Update Required? (Y/N)
21	IRRELEVANT															
20	1	ITS External Agreements	Review of CSE ITS External Agreements	**Recommendation 1.** RE: Policy: CSE should adopt a corporate directive on the subject of agreements with external parties.	Process	August-21-02	Accepted	-	ITS	[redacted]	September-30-06	September-30-06	Completed	Mission Management in IT Security life cycle manages all IT Security MOUs, MOAs and other agreements. The operational procedure detailing how this is done are completed and will be translated by 11 Jan 2007. The procedure will then be circulated for final signature which is expected in March\ 2007. Q2 E-MAIL 12-04-07 : Q2A has implemented a process to track and monitor ITS MOUs and MOAs.	-	N
20	1	ITS External Agreements	Review of CSE ITS External Agreements	**Recommendation 2.** RE: administration: responsibility for custody, control, and administration of external agreements should be centralized within CSE (or at least within ITS for ITS arrangements), and all existing agreements be reviewed immediately to establish and update status.	Process	August-21-02	Accepted	Centralized in DC IT Security area.	ITS	[redacted]	-	-	Completed	As of October 1, 2004, custody, control and administration of external agreements has been centralized within the IT Security Mission Management Group. Lifecycle review and analysis has been performed to determine follow-up action required on each agreement. Ongoing quarterly status reports will be provided.	-	N
20	1	ITS External Agreements	Review of CSE ITS External Agreements	**Recommendation 3.** RE: administration: administrative procedures should be established for registering new agreements as they are approved, for regular review and monitoring of existing arrangements throughout their active life-cycle, and for advising ITS management when follow-up action is required. The latter would include archiving documents upon termination or expiry.	Policy and guidance	August-21-02	Accepted	-	ITS	[redacted]	-	-	Completed	An operating procedure on the lifecycle review of external agreements was completed in July 2005. The scope of the procedure includes the registering of new agreements, their review, follow-up and monitoring process as well as the process for archiving expired documents. Quarterly reviews have been implemented and are briefed at the IT Security Executives meeting	-	N
[redacted]																
19	IRRELEVANT															
18	1	[redacted]	Report on [redacted]	**Recommendation 1:** RE: Extension of Services: it will be a difficult task to define the boundaries of the evaluation and limit the scope of activity for such an exercise to an acceptable level of risk. CSE ITS must continue to consider potential issues associated with "command authority" and extending [redacted] services to its client communities.	Process	August-20-01	Accepted	Covered in follow-up study [redacted]	ITS	N	-	-	Completed	-	-	N
18	1	[redacted]	Report on [redacted]	**Recommendation 2:** RE: [redacted] in reviewer's opinion, [redacted] is extremely difficult to justify within the present control framework and should be avoided. CSE ITS must determine, therefore, under what circumstances would [redacted] be approved, given the difficulty in establishing an acceptable and appropriate control framework for the use of [redacted] practices.	Business Practices	August-20-01	Accepted	Covered in follow-up study [redacted] Social engineering has not been approved for ITS activities to-date.	ITS	N	-	-	Completed	-	-	N
18	1	[redacted]	Report on [redacted]	**Recommendation 3:** RE: Treatment of Evidence: the CFIOG's Standard Authorized Activities and Procedures (SAAP) stated that when dealing with the situation where the [redacted] identifies a potential illegal activity that the information would be provided to appropriate law enforcement authorities *only if its collection was legally authorized*. Reviewer questioned implication that	Policy and guidance	August-20-01	Accepted	Covered in follow-up study [redacted] Procedures have been amended to cover this situation.	ITS	N	-	-	Completed	-	-	N
18	1	[redacted]	Report on [redacted]	**Recommendation 4:** RE: Potential Liabilities: possibility of human error and technical failure is always present in [redacted] exercises. Team might be exposed to significant and unacceptable risk unless liability has been limited by appropriate clauses in the control documents. Issues of liability for [redacted] could become a significant factor. It might be very difficult for the client to limit risk to a tolerable level. CSE should give further consideration to this issue.	Process	August-20-01	Accepted	Covered in follow-up study [redacted] Procedures have been amended to cover this area.	ITS	N	-	-	Completed	-	-	N
17	1	EPR (Phase3)	A Study of the EPR Process - Phase III: An Analysis of EPR Production and Safeguards	**Recommendation 1:** CSE must update its release criteria used to support requests for the release of Canadians names / identities.	Policy and guidance	April-06-01	Accepted	See OPS-1, Section 6.9 Suppressed Information and OPS-1-1, *Procedures for Release of Suppressed Information from COMINT*.	PC	D	-	-	Completed	New version of OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports*, released in February 2003,	-	N
17	1	EPR (Phase3)	A Study of the EPR Process - Phase III: An Analysis of EPR Production and Safeguards	**Recommendation 2:** CSE must ensure that a client's need to know a Canadian identity is readily apparent; a client must provide a clear and independent rationale to justify each request - one which can be linked to the operating program of the client department and, where a request is based upon a potential violation of a law of Canada, the appropriate citation must be provided.	Policy and guidance	April-06-01	Accepted	The particulars of the update are documented in OPS-1-1, *Procedures for Release of Suppressed Information from COMINT*.	PC	D	-	-	Completed	-	-	N
17	1	EPR (Phase3)	A Study of the EPR Process - Phase III: An Analysis of EPR Production and Safeguards	**Recommendation 3:** CSE should require clients to provide a clear indication of the intended use of the released Canadian information, and to advise CSE if the information is used for a purpose other than originally intended.	Policy and guidance	April-06-01	Accepted	See OPS-1, Section 6.9, Suppressed Information and OPS-1-1, *Procedures for Release of Suppressed Information from COMINT*.	PC	D	-	-	Completed	-	-	N
17	1	EPR (Phase3)	A Study of the EPR Process - Phase III: An Analysis of EPR Production and Safeguards	**Recommendation 4:** CSE must ensure that any Canadian identities released to clients are adequately safeguarded and protected while in the client's custody.	Policy and guidance	April-06-01	Accepted	See OPS-1-1, *Procedures for Release of Suppressed Information from COMINT*.	PC	D	-	-	Completed	-	-	N
17	1	EPR (Phase3)	A Study of the EPR Process - Phase III: An Analysis of EPR Production and Safeguards	**Recommendation 5:** CSE should be able to account for the number of Canadian identities entered into [redacted] in any given year, including the number of unique Canadian persons, organizations or corporations.	Process	April-06-01	Accepted	The yearly report on Safeguarding the Privacy of Canadians provided all this information until it was discontinued in 2003 in favour of more rigorous measurement options. This information is now contained in CSE Chief's (CCSE) dashboard metric that monitors the provision of suppressed information to SIGINT clients (used for internal CSE purposes only).	PC	D	-	-	Completed	Detailed reporting mechanisms and accountability instruments also include Management Monitoring Policy Reviews that assess the degree to which SIGINT operational areas are complying with OPS-1, and the tracking metric slated for release in the second quarter of FY 05/06; and Statistics gathered to satisfy Ministerial Authorization reporting requirements in relation to various activities.	-	N
16	1	EPR (Phase 2)	A Study of the EPR Process - Phase II: Handling Information about Canadians	**Recommendation 1:** CSE should develop documentation and training to assist its analysts in determining when to retain and use information about Canadians as defined in CPP 2010. (i.e. deemed essential versus incidental)	Process / Policy and guidance	April-06-01	Accepted	CPP 2010 has been superseded by OPS-1. See Section 6.3 of OPS-1.	PC	D	-	-	Completed	-	-	N
16	1	EPR (Phase 2)	A Study of the EPR Process - Phase II: Handling Information about Canadians	**Recommendation 2:** CSE should explore various means to segregate raw traffic containing information about Canadians used to generate EPRs	Process / Policy and guidance	April-06-01	Accepted	-	SIGINT	[redacted]	-	-	Completed		-	N

Review Number	Recommendation #	Review – Short Title (with link to TofR)	Review – Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for internal use)	CSEC Comments (for OCSEC)	Update Required? (y/n)
16	1	EPR (Phase 2)	A Study of the EPR Process - Phase II: Handling Information about Canadians	**Recommendation 3:** CSE should implement formalized procedures for reviewing / managing client access to EPRs.	Process / Policy and guidance	April-06-01	Not Accepted	Workload would be untenable due to changing client needs.	-	-	-	-	N/A	CSE procedure OPS-5-6 Client Access to SIGINT Information, addresses the provision of SIGINT to organizations, but not down to the client level. However, an audit capability exists where abuses are suspected. Random checks are also possible. Particularly sensitive reporting is already subject to special controls and selective distribution.	-	N
16	1	EPR (Phase 2)	A Study of the EPR Process - Phase II: Handling Information about Canadians	**Recommendation 4:** CSE should accelerate the establishment of its records management authorities for its operational holdings and establish, in parallel, retention and disposal schedules for these same holdings.	Process / Policy and guidance	April-06-01	Accepted	An RDA for ITS obtained in FY 03/04. RDA for FI obtained in December 2004. SIGINT RDA in progress and expected to be completed by end of second quarter FY 05/06. This is also part of the larger IM plan (target date FY 07/08). Retention schedules for s.16 traffic are addressed in OPS-1-11.	CIO	-	March-31-08	0000-00-00	Completed			N
15	1	Policy System	Policy System Review	**Recommendation 1:** A dedicated corporate database or repository for CSE policies would be beneficial and should be implemented on a priority basis	Process	September-13-00	Accepted	Operational Policies available at single web address. Corporate policy repository also available at single web address.	PC	D	-	-	Completed	-	-	N
15	1	Policy System	Policy System Review	**Recommendation 2:** CSE should dedicate additional resources to policy development	Process	September-13-00	Accepted	Two additional FTEs have been added to D2's office.	PC	D	-	-	Completed	-	-	N
15	1	Policy System	Policy System Review	**Recommendation 3:** Deficiencies remaining from previous reviews should be re-examined at a later date.	N/A	September-13-00	None	-	-	-	-	-	N/A	-	-	N
14	1	External Review of ITS	Findings of an External Review of CSE's ITS Program	**Recommendation 1:** CSE's 2000-2001 internal review plan should include a review of CSE's ITS agreements with external parties. Through this review CSE should be able to better assess the authorities, obligations, dependencies and liabilities involved in these relationships [redacted], and Entrust (PKI licences).	Process	June-15-00	Accepted	Report (no. 20) submitted to the Minister 21 August 2002.	ITS	[redacted]	-	-	Completed	-	-	N
13	1	Internal Investigations and Complaints (follow-up)	Internal Investigations and Complaints: Follow-up Study	**Recommendation 1:** Commissioner will re-examine CSE's progress in implementing HR mechanisms and practices to address employee issues related to hiring and release when conducting the Policy System Review.	N/A	May-10-00	Accepted	See Review # 28 on Internal Security at CSE.	-	-	-	-	Completed	-	-	N
12	IRRELEVANT															
11	1	Selection [redacted]	A Study of Selection [redacted] An Overview	**Recommendation 1:** CSE is encouraged to continue to advance initiatives to identify and anticipate better the technical characteristics of Canadian communications [redacted] These initiatives will likely improve CSE's ability to refine [redacted] and advance the technical means its undertakes to ensure that the privacy of Canadian communications remains protected in this rapidly changing environment.	Process	May-10-00	Accepted	This has been addressed by technology and CSE legislation.	SIGINT	[redacted]	-	-	Completed	-	-	N
10	0	EPR	A Study of the End-Product Reporting (EPR) Process Phase I	No recommendations.	N/A	December-08-99	None Required	-	-	-	-	-	N/A	-	-	N
9	1	[redacted]	[redacted]	**Recommendation 1:** CSE should not participate in any operational activity, even in a supporting capacity, without its customary advice from Justice Department's legal counsel in advance of its involvement.	Process / Legal	December-08-99	Accepted	-	-	-	-	-	Completed	-	-	N
8	0	[redacted] program	A Study of the [redacted] Collection Program	No recommendations.	N/A	November-19-99	None Required	-	-	-	-	-	N/A	-	-	N
7	0	How we Test	How We Test	No recommendations.	N/A	June-14-99	None Required	-	-	-	-	-	N/A	-	-	N
6	1	COMSEC	Controlling Communications Security (COMSEC) Material	**Recommendation 1:** A log to identify and track the [redacted] produced in [redacted] Group is maintained and reviewed by [redacted] Group's user services personnel. Access to the log operates under Two Person Integrity. From time to time, the log should be randomly verified by employees not involved in the production of [redacted]	Policy and guidance	May-06-99	Accepted	The requirement for Two Person Integrity is covered in ITS-01 and MG-14.	ITS	[redacted]	-	-	Completed	-	-	N
6	1	COMSEC	Controlling Communications Security (COMSEC) Material	**Recommendation 2:** CSE should provide client departments timely feedback on obvious changes in COMSEC material usage patterns that could lead to the identification of unauthorised usage of equipment, as were as early detection of lost or missing components.	Process	May-06-99	Accepted	Implemented as a [redacted] responsibility.	-	-	-	-	Completed	-	-	N
5	IRRELEVANT															
4	1	Internal Investigation & Complaints	Internal Investigations and Complaints	**Recommendation 1:** CSE should ask DND to provide all information on those employees it is considering hiring in order to be aware of personnel-related problems that may have existed.	Process	March-10-98	Accepted	See follow up study (# 13).	CS	[redacted]	-	-	Completed	-	-	N
3	IRRELEVANT															

Review Number	Recommendation	Review – Short Title (with link to ToR)	Review – Full Title	Review Recommendations	Recommendation Category	Review Report Date (with link to final report)	Recommendation Acceptance	CSEC Management Response	Business Line Responsible	Group Responsible	Due Date	Actual Completion Date	Status	CSEC Comments (for Internal Use)	CSEC Comments (for OCSEC)	Update Required? (Y/N)
3	IRRELEVANT															
2	1	OPS with lawfulness	Operational Policies with Lawfulness Implications	**Recommendation 1:** CPP 2010 and DGP/D 2102 should be issued to CSE as Ministerial Directives	Authorities	February-06-98	Accepted	See Ministerial Directives: CSE, *Privacy of Canadians*, June 19, 2001; CSE, *Support to Law Enforcement and National Security Agencies*, June 19, 2001.	-	-	-	-	Completed	-	-	N
[redacted]																
1	IRRELEVANT															
1																

Year	Review Number	Review Short Title	Review Title	Findings	Action detailed in the letter to the MND	Review Report Date	Business Line	Area	Due Date	Status	CSEC Comments (for Internal Use)
2014-2015											
	91	[redacted] Review	Review of CSEC [redacted] Activities [redacted] Interception) under Foreign Signals Intelligence Ministerial Authorizations								
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 12: "CSE's failure to minimize DNR and DNI metadata, and its failure validate identifiers prior to sharing DNI metadata with international partners, raise legal questions that need to be explored in further detail." (p.46)		March-31-15					
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 11: "CSE proactively suspended the sharing of both DNR and DNI metadata with Second Parties in order to protect the privacy of Canadians while developing a solution to the problems it encountered in this area." (p.45)	None	March-31-15					
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 10: "During the course of the review, CSE discovered that DNI being shared with Five Eyes was not subject to proper validation or minimization, in accordance with CSE policy and the Ministerial Directive." (p.42)		March-31-15					
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 9: "CSE's system for sharing DNI metadata with Second Parties was poorly understood by the organization and lacked a proper record-keeping process." (p.39)		March-31-15					

	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 8: "CSE's system for minimizing [redacted] DNR metadata was decentralized and lacked appropriate control and prioritization." (p.38)		March-31-15					
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 7: "CSE lacked a proper means of verifying whether minimization scripts were functioning properly for [redacted] DNR metadata shared with Five Eyes partners, and lacked a proper record-keeping process." (p.37)		March-31-15					
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 6: "During the course of the review, CSE discovered that [redacted] DNR metadata being shared with Five Eyes partners was not being minimized properly, contrary to the Ministerial Directive and to operational policy." (p.33)		March-31-15					
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 5: "CSE's IP Profiling Analytics tradecraft, which was the subject of an unauthorized disclosure, was authorized under 273.64(1)(a) of the NDA, and CSE took measures to protect the privacy of Canadians in undertaking this activity." (p.30)	None	March-31-15					
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 4: "The 2011 Ministerial Directive on Collection and Use of Metadata lacks clarity regarding the sharing of certain types of metadata with Second Parties, as well as other aspects of CSE's metadata activities." (p.28)		March-31-15					

	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 3: The Canadian legal landscape has changed since the Commissioner's office last conducted an in-depth review of CSE's collection and use of metadata.		March-31-15	DLS	DLS		Ongoing	As to Finding #3 and the proposed action, DLS has been looking at the 'seminal' Solicitor-Client Privilege Solicitor-Client Privilege Solicitor-(We are working on other parts – our drivers are the BCCLA litigation and the ever evolving legal landscape.
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 2: Metadata collection and analysis has evolved considerably since the Commissioner's last in-depth review of metadata activities, and metadata remains critical to all aspects of CSE's SIGINT mission.	None	March-31-15					
	90	SIGINT Metadata Review	Review of CSE's use of Metadata in a Signals Intelligence Context	Finding no. 1: CSE was forthcoming with information and assistance, both proactively and in response to specific requests of the Commissioner's office.	None	March-31-15					
	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2002	Finding no. 11: Policy Compliance Monitoring CSE managers routinely and closely monitored Active Network Security Testing and Cyber Defence Operations activities for compliance and protection of the privacy of Canadians.	None	April 8 2015					

	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2003	Finding no. 10: Policies and Procedures Relating to the Retention of Private Communications (2) CSE policy does not provide clear guidance on the circumstances, if any, in which a cyber defence analyst can retain a one-end Canadian e-mail involving malicious code that is not linked to an incident or used in a report, that is an "orphaned event".	N/A	April 8 2015					
	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2004	Finding no. 9: Policies and Procedures Relating to the Retention of Private Communications (1) Policies and procedures relating to the retention of private communications were not followed in some instances; however, it is a positive development that CSE made system improvements intended to promote and permit CSE to demonstrate compliance.	The Commissioner will examine these systems in a future review to ensure the improvements are effective.	April 8 2015					
	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2005	Finding no. 8: Awareness of Personnel Interviews with and observations of IT Security managers and other employees demonstrated that they are knowledgeable about policies and procedures aimed at compliance with the law and the protection of the privacy of Canadians.	None	April 8 2015					

	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2006	Finding no. 7: Appropriateness of Policies and Procedures — Compliance with the Law and Protection of the Privacy of Canadians CSE has sufficient policies and processes to satisfy the legal requirements not to direct its IT security interception activities at a Canadian or any person in Canada and to protect the privacy of Canadians in the use and retention of private communications and intercepted information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks; however, some policies and procedures could be improved.	The inclusion of guidance in CSE policies and procedures on CDO record keeping requirements and practices regarding cyber events and incidents, that include a PC, would enhance CSE's ability to demonstrate complaince and the protection of the privacy of Canadians.	April 8 2015					
	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2007	Finding no. 6: Metrics Relating to Private Communications CSE reporting to the Minister of National Defence and Chief of CSE on metrics relating to private communications unintentionally intercepted during the conduct of authorized cyber defence operations under ministerial authorizations was not completely accurate; however, CSE identified and addressed the error.	None	April 8 2015					

	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2008	Finding no. 5: Ministerial Requirements Based on the information reviewed and the interviews conducted, CSE carried out its Active Network Security Testing and Cyber Defence Operations activities in accordance with the ministerial authorizations and ministerial direction.	None	April 8 2015					
	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2009	Finding no. 4: Cyber Defence Operations Private Communications CSE's practice —Solicitor-Clier Solicitor-Client Privilege	**I therefore recommend** that CSE reporting to the Minister on PCs unintentionally intercepted under MAs should highlight the important differences between one-end in Canada e-mails intercepted under CDO and private communications intercepted under foreign signals activities, including the lower expectation of privacy attached to the private communications intercepted under CDO	April 8 2015					

	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2010	Finding no. 3: IT Security Ministerial Authorizations Paragraph 273.65(3) of the NDA does not seem to reflect CSE's activities because CSE undertakes activities other than those considered in "the circumstances specified in paragraph 184(2)(c) of the Criminal Code".	Since CSE rarely acts in the circumstances set out in par. 184(2)© of the Criminal Code, it can be argued that an MA issued under subsection 273.65(3) of the *NDA* would not include CSE's primary cyber defence activities undertaken under an IT security MA. Therefore, CSE should encourage the government to amend subsection 273.65(3) of the National Defence Act as soon as practicable to remove any ambiguities respecting CSE's authority to conduct IT security activities that risk the interception of private communications.	April 8 2015					
	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2011	Finding no. 2: IT Security Systems that Promote Privacy Protection CSE takes measures in the design of its IT security systems and databases to promote compliance with the law and the protection of the privacy of Canadians.	None	April 8 2015					

	89	ITS ANST/CDO 2013	Combined review of CSEC Active Network Security Testing (ANST) and Cyber Defence Operations (CDO) activities during the period of 2009-2010, 2010-2011 and 2011-2012	Finding no. 1: Compliance with the Law Based on the information reviewed and the interviews conducted, CSE Active Network Security Testing and Cyber Defence Operations activities were appropriately authorized and were conducted in accordance with the law, as interpreted by the Department of Justice Canada.	None	April 8 2015					
	88	PIF and MPER 2014	Annual review of the Communications Security Establishment (CSE) Privacy Incident File (PIF) and Minor Procedural Errors Report (MPER) for calendary year 2014	No findings	None	March-31-15					
	87	Disclosures 2014	Annual review of disclosures, by the Communications Security Establishment (CSE), of Canadian identity information (CII) from CSE end-product reports disseminated to clients	No findings	None	March-12-15					

	86	SIGINT MAs	Annual Combined Review of Foreign Signals Intelligence Ministerial Authorizations for 2013-2014	No findings	None	March-03-15					
	85	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	Finding no. 9: 2008 DAEE Audit Report Action The recommendations of the 2008 DAEE audit report have been actioned.	None	March 19 2015					
	85	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	Finding no. 8: Management Control Framework CFIOG officers in charge and supervisors routinely and closely monitor CSD activities to make certain the activities comply with governing authorities.	None	March 19 2015					
	85	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	Finding no. 7: Awareness of Personnel to Policies and Procedures CSD employees interviewed and observed were aware of relevant policies and procedures, including those relating to the protection of the privacy of Canadians, and their application to routine CSD activities.	None	March 19 2015					

	85	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	Finding no. 6: CSD Establishing Documents Inconsistent and Not Necessarily Complete There is an inconsistent set of documentation covering the various CSDs; however, they do not appear to present any impediments to the operation, oversight or compliance of the individual CSDs.		March 19 2015					
	85	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	Finding no. 5: Appropriateness of Policies and Procedures in Place Established policies and standing operating procedures are in place to both guide the CSD staff and provide a means for the efficient and effective day-to-day process that appears to be the norm.	None	March 19 2015					
	85	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	Finding no. 4: Compliance with Ministerial Direction Based on the information received, the activities observed, and the interviews conducted, the CSDs conduct their activities in accordance with applicable ministerial direction.	None	March 19 2015					
	85	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	Finding no.3: CSE Compliance Monitoring CSE ensured that the SIGINT activities of the CSD's complied with the law.	None	March 19 2015					
	85	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	Finding no. 2: Protection of privacy The activities, as they are currently carried out by the CSDs, do not present privacy implications.	None	March 19 2015					

	85	CAF CSD	Review of the Canadian Armed Forces Cyber Support Detachments	Finding No. 1: Compliance with the Law Based on the information received, the activities observed, and the interviews conducted, the CSDs conducted their activities in compliance with the law.	None	March 19 2015					
	84	IRRELEVANT									
	84										
	84										

	84	IRRELEVANT									
	84										
	84										
	84										
	83	Spot Check Review Fall 2014	"Spot check" review of SIGINT private communications used or retained by CSE	One finding: CSE is taking action to quickly implement the recommendations of the Commissioner's March 2014 review of SIGINT MAs and PCs	None	December 11 2014					
	82	Spot Check Review Summer	"Spot check" review of SIGINT private communications used or retained by CSE	One finding: CSE is taking action to quickly implement the recommendations of the Commissioner's March 2014 review of SIGINT MAs and PCs	None	August-14-2014					
2013-2014											
	81	PIF 2013		No findings		March 1 2014					

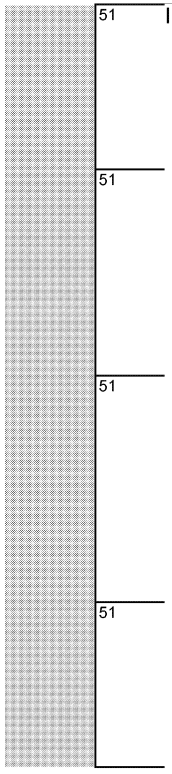
	80	SIGINT Mas 2013		Finding no. 10: Essentiality of Used or Retained Private Communications (4) A number of analysts retained private communications that had once been, but were no longer, essential to international affairs, defence or security; despite regular, written reminders to review and mark for deletion any private communications that were no longer essential, these private communications were retained — in some cases, for several months — until just before the expiration of the ministerial authorizations and prior to associated reporting to the Minister.	Addressed by Recommendation #4 from Report: SIGINT to ensure that all analysts review their retained private communications quarterly, commencing at the end of the next quarter.	March 1 2014					
	79	Disclosures 2013		6 Findings: No specific follow up action is required.		March 1 2014					
	78	Office of Counter Terrorism 2012		There were 8 findings but no specific follow up action is required.		October 1 2012					
	77	Policy Compliance Study 2012-2013		Finding no. 1: "Subsequent to the 2009 CSEC Audit of OPS-1-8 Compliance CSEC SIGINT and IT Security have taken significant actions, namely the implementation of a new policy framework for policy compliance monitoring and detailed operational instructions, training and testing, and a number of new related activities"	Action on Finding no. 2: Since the production of the study report both SPOC and IPOC have migrated their compliance monitoring records into CERRID 2.0 and have adopted consistent naming conventions within their own areas. Non-compliance incident tracking documentation is in place in both areas which will facilitate swifter retrieval for metrics of non-compliance incidents.						

	76	Second Party Info Sharing		No findings that require action (all addressed by responses to the report's recommendations).		July-17-13					
	75	AEN Additional Information		No findings						
2012-2013										
	74	SIGINT MAs 2011-2012		No findings that require action.		March-28-13				
	73	PIF 2012		No findings that require action.		March-23-13				
	72	DCII V 2012		No findings that require action.		March-18-13				
	71	[redacted] Review		Finding 5: CSEC did not adequately protect the privacy of a Canadian – [redacted] – in three exchanges of information in [redacted] and one in [redacted] however, since that time, CSEC has taken appropriate actions for accountability and to prevent re-occurrences of similar privacy incidents.		February-15-13	SIGINT				As noted in the Commissioner's report, CSEC has committed to promulgating guidance for SIGINT employees with respect the sharing of Canadian identity information with Second Parties.
	71	[redacted] Review		Finding 6: The absence of certain historical information in CSEC's targeting database and tool – [redacted] – limited the Commissioner's ability to assess the lawfulness of CSEC's activities relating to [redacted] and could also affect review of other activities of CSEC.		February-15-13	SIGINT				CSEC anticipated at the outset of this review that, given its focus on historical records, retrieval of information would be problematic. This was communicated to the Commissioner's Office. The targeting systems used by CSEC during the period under review were not designed to keep a history of targeting activity, but would indicate which selectors were targeted at the time of a query. As noted in Finding 7, CSEC is already taking action to address this issue.

71	[redacted] Review		Finding 7: During the period under review, CSEC did not always retain a history of targeting activity; however, CSEC is taking actions to ensure the availability of information about targeting and selector management that is required for accountability and to demonstrate compliance with the law.		February-15-13	SIGINT				As noted in this finding, CSEC is already taking action to address this issue.
70	Non-MA CDO		No findings that require action.		January-14-13					
69	DIFTS		No findings that require action.		November-20-12					
68	2011SIGINT MAs 2009-10	Review of CSEC's 2009-2010 foreign Intellilgence Ministerial Authorizations	Finding 5: "…did not address reccomentdation no. 1 in the Commiioner's February 2009 review of CSEC's [redacted] Finding 8: "Changes made by CSEC to the time period for the ministeral authorizations and to technology negatively impacted the Commissioner's ability..." Finding 9: Metrics respecting the number of communications...sent to its Second Party partners were not readily available." Finding 10: [redacted] issue recommendation 2 from last SIGINT MA review not addressed		March-30-12		none		Letter sent to C'r from MND	CSEC's position has not changed. CSEC has nevertheless aggreed to count PCs in this context and report the nuber to the Minister to better inform him
67	interim report	update on an ongoing review of CSEC's foreign signals intelligence sharing with [redacted] partners	No findings.							
66	PIF 2011		No findings.		March-20-11					

65	DIAC IV (2011)		No findings.		March-13-11					
64	COPCC		Finding 5: Operational instructions provide limited instruction specific to the functioning of the COPCC.	It is a positive development that CSEC has recognized this gap and is developing an operation instruction respecting the activities of the COPCC.	[redacted]					
63	Retention, disposal of data		Finding 7: "… certain language in policy should be clarified". Finding 8: "The parts of OPS-1-11 concerning retention and disposal of transitory records and those records used in reporting are confusing and should be clarified. Finding 9: "To avoid confusion, the use of terminology relating to retention and disposal activities used by the SIGINT and IT Security Programs should be reconciled and made consistent".		December-22-11					
62	PIF 2010				July-04-11					
61	T&SM		Total of 20 findings, 1 tied to the only recommendation.	Tied to the recommendation.	March-15-11				On track	April 2012: Draft guidance has been prepared and is undergoing consultation and revision. It is expected to be finalized in this fiscal year.
60	SIGINT MAs		Total of 15 findings, three tied to a recommendation. A separate finding may be considered negative: "The descriptions of the five SIGINT collection program activities in the request memoranda to the Minister are inconsistent and minimal."	Only one recommendation accepted. On the separate finding: BN to ExCom noted: CSEC will consider this feedback during the next MA renewal period	February-25-11	DGPC	B	2011 MA renewal period	Completed	May 2012: CSEC maintains its position that [redacted] does not constitute a private communication and therefore does not trigger a legal reporting requirement. Nonetheless, to support the Minister with additional contextual information, CSEC intends to begin compiling the number of recognized one-end Canadian emails [redacted] that are retained by CSEC on the basis that they are essential to international affairs, defence or security.
59	DIAC III		No findings.	No action required.	February-21-11					

	58	ANST		Total of 10 findings listed in Annex A of the final report. None require action.	No action required.	February-14-11					
	57	Contact Chaining		Total of 5 findings (listed in Annex A of the final report). None reqire action.	No action required	December-16-10				N/A	
	56	CND MA Review (October 2010)		Total of 18 findings (listed in Annex A of the final report). None require action.	No action required	October-18-10				N/A	
	55	Regular Privacy Review (DIAC II)		Total of 2 findings. None requring action.	No action required.	February-16-10	-	-	-	Completed	[redacted]
	54	Afghanistan Mas		Total of 6 findings. None requiring action	No action required.	January-18-10	-	-	-	N/A	
	53	ITS Study	A Study of the CSEC's Information Technology (IT) Security Activities Not Conducted Under a Ministerial Authorization (MA)	None. Only 5 findings	No action required.	June-11-09	-	-	-	N/A	
	52	NAF[redacted]A	CSEC's [redacted] Network Analysis and Prioritization and [redacted] Activities	**Total of 7. None requiring action**	No action required.	March-12-09	-	-	-	N/A	



51 IRRELEVANT

51

51

51

51

51

51

51

IRRELEVANT

A-2017-00017--04015

50	[redacted]	Review of CSEC Signals Intelligence Activities Conducted Under Ministerial Directive & Authorization - [redacted]	**Finding no. 4:** While the practices in place at the working level demonstrate that CSEC assesses the threats, risks and vulnerability associated with proposed [redacted] operations, CSEC did not comply with the requirement of the [redacted] ministerial directive to *define* in procedures "appropriate threat, risk and vulnerability *thresholds* for both the activity and personnel involved".	**Tied to Recommendation 1.** *Please provide an update for the recommendation only since the finding and recommendation are linked.*	March-03-09	-	-	December-22-09	38899	N/A
50	[redacted]	Review of CSEC Signals Intelligence Activities Conducted Under Ministerial Directive & Authorization - [redacted]	**Finding no. 7:** Other than the referenced legal foundation documents, no other material was identified as providing guidance as to what legal concerns and restrictions had been identified as being relevant during the consideration of a proposed [redacted] technique.	Tied to Recommendation 2 and 3. *Please provide an update for the recommendation only since the finding and recommendation are linked.*	March-03-09	-	-	December-22-09	0	0
50	[redacted]	Review of CSEC Signals Intelligence Activities Conducted Under Ministerial Directive & Authorization - [redacted]	**Finding no. 8:** No issues or concerns were identified related to consultation and cooperation with involved agencies. Procedures, approval processes and agreements were found to be in place allowing CSE to be found compliant with this expectation. It is suggested that consideration be given to adding a reference in the [redacted] SOP to [redacted]		March-03-09	SIGINT	[redacted]	December-22-09	Completed	SPOC - March 2011: The deconfliction process is referenced in the latest [redacted] SOP, dated 29 November 2010 (para 3.10).

50	[redacted]	Review of CSEC Signals Intelligence Activities Conducted Under Ministerial Directive & Authorization - [redacted]	**Finding no. 10:** CSEC has not documented characteristics of a [redacted] operation that would cause it to be considered as being "particularly sensitive" and having "significant risk".	**Tied to Recommendation 4.** *Please provide an update for the recommendation only since the finding and recommendation are linked.*	March-03-09	-	-	December-22-09	39172	Completed
49	[redacted]	CSEC's Foreign Intelligence Activities Conducted under the [redacted] Ministerial Authorizations	**Finding no. 2:** With respect to paragraph 5 of the 2005-2006 [redacted] MA, CSEC did not meet the expectation to report to the Minister a [redacted] in the interception of private communications".	"in the future, the Chief will bring such issues to the MND attention. In addition, as per OCSEC's recommendation, the Chief will also indicate to the MND the absence of any "serious issues" in the accountability report submitted upon expiration of the MA.	January-13-09	PC	B	-	Completed	B - April 09: In his report to the MND on 2008 SIGINT activities under MA, the CCSEC stated in his cover letter that no serious issues arose under any of the Mas, and will next year incorporate a separate statement on "serious issues identified or not identified" for each MA in the attached reporting annex.
49	[redacted]	CSEC's Foreign Intelligence Activities Conducted under the [redacted] Ministerial Authorizations	**Finding no. 5:** Assessing the foreign intelligence value of reports based on private communications is difficult because it is only based on client feedback which is not always received. We encourage CSEC to introduce a greater degree of rigour to this process to yield a better assessment of the FI value of the reports.	The chief agrees that the current feedback system does not always provide with the most complete information, but points out, however, that past experience with [redacted] Moreover, EPRs are not identifiably linked to these PCs, which makes it impossible for the client to comment directly on its value.	January-13-09	SIGINT	SPOC	-	Completed	SPOC - April 09: As per CCSE comment, it is difficult to judge the value of the FI value of reports based on private communications since clients are unaware of the specifics related to the source traffic. Note that, on a broader scale, SIGINT is striving to enhance its feedback mechanisms.

49	[redacted]	CSEC's Foreign Intelligence Activities Conducted under the [redacted] Ministerial Authorizations	**Finding no. 8:** CSEC did not meet condition 4(d) of the 2006-1007 [redacted] MA because the [redacted] MA accountability report was not received by the Minister until one year after the MA expired.	"The Chief is committed to ensuring that the MA accountability report is produced by CSEC in a more expeditious manner".	January-13-09	PC	B	-	Completed	B- April 09: The 2008 [redacted] reporting letter was signed by the CCSEC and forwarded to MND on 24 April 2009, thus honouring this committment.
49	[redacted]	CSEC's Foreign Intelligence Activities Conducted under the [redacted] Ministerial Authorizations	**Finding no. 9:** For those [redacted] MA accountability reports submitted to the Minister during the review period, CSEC has fulfilled all the conditions in the MAs, with the exception of the reporting requirement concerning any serious issue.	**Tied to Recommendation 1.** *Please provide an update for the recommendation only since the finding and recommendation are linked.*	January-13-09	-	-	-	39172	Completed
48	DIAC	Disclosure of information about Canadians to Government of Canada clients	**Total of 3. None requiring action.**	No action required.	November-13-08	-	-	-	N/A	-
47	[redacted] MA	CSEC's Activities Conducted Under the [redacted] Ministerial Authorizations	**Finding no. 4:** [redacted]	[redacted]	June-11-08	PC	B	December-30-08	Completed	[redacted]

47	[redacted] MA	CSEC's Activities Conducted Under the [redacted] Ministerial Authorizations	**Finding no. 6: Management of Selectors:** Pending the development of an automated system, we question how CSEC can confirm that selectors (proposed by CSEC or by a Second Party) remain valid, directed at a foreign entity located outside Canada, and consistent with a FI priority of the Government of Canada.	CSEC agrees that the present system does not facilitate annual reviews of selectors. Consequently, CSEC is developing an automated system, which will require that selectors are reviewed and validated annually. This system will be implemented by the end of May 2009.	June-11-08	SIGINT	SPOC	May-30-09	Completed	SPOC - April 09: The automated validation system was implemented and launched on 2 April 2009. Any new selectors will automatically require validation by the analysts on an annual basis (i.e., justification, location, nationality and GCR associated with the selector must be re-validated). Any new selectors that are not re-validated on an annual basis are automatically de-targeted. In order to ensure existing selectors of value are not inadvertently de-targeted, the system will provide analysts with a six-month grace period to re-validate "expired" selectors. Upon the end of the grace period, the expired selectors which were not re-validated will be de-targeted.
47	[redacted] MA	CSEC's Activities Conducted Under the [redacted] Ministerial Authorizations	**Finding no. 7: Private Communications Shared with the Second Parties:** Reporting to the Minister the number of private communications recognized by the Second Parties and obtained as a result of CSEC collection shared with the Second Parties would enhance accountability by providing an increased understanding of the number of intercepted private communications, and would therefore enhance the protection of the privacy of Canadians.	CSEC is working with our partners on the development of an automated solution that would integrate policy compliance features in the design of future SIGINT systems. In the interim, mutual policy and reporting arrangements have been agreed to with Second Parties to ensure the privacy of our citizens. Since 2005, for example, [redacted]	June-11-08	SIGINT	SPOC	-	Completed	SPOC - April 09: The Management response on this finding was not fully coordinated. Automated solutions for policy compliance are not expected to track CSE-collected private communications recognized by 2nd party partners. Rather, those mechanisms are being developed for other aspects of the SIGINT system--to ensure compliance in targeting, for example. **October 2010** (SPOC): There is no further update to this item - the statement provided in April 2009 was intended to explain that an automated policy solution for private comms recognized by 2nd parties is not possible at this time. Instead, we rely on mechanisms and processes that we share with 2nd parties on how private comms and/or information about Canadians shoudl be handled. SIGINT considers this item closed.

47	[redacted] MA	CSEC's Activities Conducted Under the [redacted] Ministerial Authorizations	**Finding no. 8: Deletion of Recognized Non-Essential Private Communications in all Systems:** The need to ensure that all copies of recognized non-essential private communications are destroyed should be taken into consideration as CSEC's collection systems are modified or new systems are designed.	CSEC has included this feature in its new common traffic repository, which will be launched by the end of December 2008. All traffic will eventually be held in this single data repository, eliminating risks associated with having multiple copies. In the interim, staff have been directed toe ensure that all copies of non-essential PCs are destroyed in all databases.	June-11-08	SIGINT	SPOC	December-30-08	Completed	SPOC - April 09: The Common Traffic Repository has been implemented, through a phased approach. As a result of the move to CTR, analysts are only required to annotate traffic in a single database. For that traffic which is not yet part of the CTR [redacted] fax traffic), a synchronization function has been implemented so that analysts are not required to annotate in multiple databases.
46	P&T	Report to the CSE Commissioner on Protecting Privacy: Review on CSEC's Acquisition and Implementation of Technology per Subsection 273.64 (2) of the National Defence Act	**Finding no. 10:** During the period under review, CSEC did not give corporate approval to the [redacted] Standard Operating Procedures.	OCSEC is aware that this has since been addressed in the new policy instruments and their approval process.	June-11-08	ITS	[redacted]	-	Completed	OCSEC is aware that this has since been addressed in the new policy instruments and their approval process.
46	P&T	Report to the CSE Commissioner on Protecting Privacy: Review on CSEC's Acquisition and Implementation of Technology per Subsection 273.64 (2) of the National Defence Act	**Finding no. 11:** CSEC did not give corporate approval to policy or procedures describing the process to release suppressed information found in IT Security reports.	Already addressed through the IT Security business resumption and the revised OPS-1-14.	June-11-08	ITS	CDSO	-	Completed	Already addressed through the IT Security business resumption and the revised OPS-1-14.

45	[redacted] MD & MA	A Review of CSE Intelligence Activities Conducted Under Ministerial Directive & Authorization – [redacted]	**Finding no. 2:** While CSE has generally adhered to many of the concepts detailed in the [redacted] requirements, the rigor we expected to find was lacking in business processes. Further, the record of satisfaction of key requirements found within the program files was inadequate.	Tied to Recommendation 1. *Please provide an update for the recommendation only since the finding and recommendation are linked.*	March-28-08	-	-	-	39082	Completed
45	[redacted] MD & MA	A Review of CSE Intelligence Activities Conducted Under Ministerial Directive & Authorization – [redacted]	**Finding no. 3:** CSE should assess whether a [redacted] support program needs to be made available to [redacted] programs, such as [redacted]	CSEC agreed with the Commissioner's office and instituted program changes prior to the completion of the review. We are in the process of developing guidance on [redacted] which will list requirements for managing such [redacted] We expect drafts of these documents by the end of September.	March-28-08	SIGINT	SPOC	-	Completed	**March 2011** (SPOC): CSOI-F-1, CSEC Special Operations Governance Document, was signed off in early 2009, and promulgated in November 2010.
45	[redacted] MD & MA	A Review of CSE Intelligence Activities Conducted Under Ministerial Directive & Authorization – [redacted]	**Finding no. 4:** The absence of an approved contingency and exit strategy is in contravention of the expectation of the [redacted] MD. **Finding no. 8:** [redacted] CONOP is required as a critical component of the required explicit internal management framework.	The Commissioner reported that CSEC lacked an approved Concept of Operations document, in addition to a contingency plan and exit strategy. CSEC is currently developing all three of these documents with completion planned for the end of this month.	March-28-08	SIGINT	SPOC	June-30-08	Overdue	SPOC - April 09: Documents are in draft. **October 2010** (SPOC): The documentation is partially completed [redacted] Operations Guidelines has been created and a framework has been agreed upon for its maintenance. [redacted] and the document may be updated as circumstances [redacted] change. Contingencies and Exit strategies are covered [redacted] but under contruction [redacted] The document is reviewed at a minimum yearly but generally as circumstances change enough to warrant an update. **Sep 2011** (SPOC): Finding #4: The contingency and exit strategy is in draft. **Sep 2011** (SPOC): Finding #8: The [redacted] CONOP is in draft.

45	[redacted] MD & MA	A Review of CSE Intelligence Activities Conducted Under Ministerial Directive & Authorization – [redacted]	**Finding no. 5:** The information provided suggests that CSE has not consistently adhered to the requisite degree of consultation and level of approval required by the Approval Framework as stated in the [redacted] MD. Further, it appears that no attempt was made to quantify what is meant by "costs and risks that are similar to those of currently approved initiatives".	CSEC policies and procedures are evergreen and will be refined to address the identified shortcomings.	March-28-08	PC	D2	-	Completed	D2 - April 09: OPS-1-13 will be amended concurrently with SIGINT MA renewals (which expire on 22 December 2009, so target date is 23 December). I assume that this will be addressed (it wasn't for the December 2008 revision, not sure why that is since the finding had been communicated to us). **October 2010** (D2): An Activity Authorization Request (AAR) is prepared by two levels of operations and is reviewed and approved by two different Directors (SIGINT Requirements and Global Access). These levels of approval appear in the version of OPS-1-13 that was effective 23 December 2009). Marked as completed November 2010.
45	[redacted] MD & MA	A Review of CSE Intelligence Activities Conducted Under Ministerial Directive & Authorization – [redacted]	**Finding no. 13:** The absence of any requirement to document the reasonable grounds upon which an analyst has determined that a selector is directed at foreign entities located outside Canada and is consistent with the GoC intelligence priorities leaves no means to audit and review approved selectors and thus renders OCSEC incapable of verifying compliance with this condition. **Finding no. 23:** CSE is not using available technology and information effectively to assist in the identification of PCs which impacts on the ability to audit and review the [redacted] collection program for reporting to the Minister. **Finding no. 28:** Analysis of the content of the required automated database of selectors does not provide the means to verify that CSE has grounds to believe that all intercept of private communications is related to foreign entities located outside Canada.	The aforementioned measures to better document the rationales for our decision-making processes will include a particular focus on targeting/selectors and private communications. Guidance has already been issued regarding the documentation and justification necessary for targeting selectors. Also, SIGINT is developing the required tools to implement a single automated database of selectors this fall.	March-28-08	SIGINT	SPOC	September-30-08	Completed	SPOC - April 09: CSEC promulgated CSOI-4-4, *Targeting and Selector Management Using* [redacted] *National SIGINT Systems for Intelligence Reporting Purposes*, on 11 March 2009. These instructions address the documentation requirements associated with determining whether or not to target a selector. Analysts have been informed that all selectors that are submitted for targeting must be recorded in the target knowledge base (TKB). CSEC is moving towards a single automated database for selectors.

	45	[redacted] MD & MA	A Review of CSE Intelligence Activities Conducted Under Ministerial Directive & Authorization – [redacted]	**Finding no. 26:** CSE is not making best use of available technology to effectively limit intercept to only outside Canada.	Unfortunately, CSEC has not identified any technology that can be used to satisfy the requirement above. We continue to examine emerging technologies and their potential applications to address all of our requirements, including those that OCSEC has identified in its reviews. In the meantime, we are focusing our efforts on recruiting analysts with the required competencies, delivering an effective training program, developing effective tools to support CSEC analysts in identifying private communications and ensuring that sufficient checks and balances are in place for privacy protection.	March-28-08	SIGINT	SPOC	-	N/A	SPOC - April 09: No change from previous update. We do not see this as an achievable goal, given the nature of the GII.

45	[redacted] MD & MA	A Review of CSE Intelligence Activities Conducted Under Ministerial Directive & Authorization – [redacted]	**Finding no. 34:** CSE should assess whether the necessity to maintain strict need to know requires greater rigor in the recording of events, decisions, analysis, agreement and processes. **Finding no. 35:** Based upon the information provided, an evidentiary record of compliance with the imposed conditions (NDA/MA) cannot be found within the records of CSE.	CSEC is re-examining its business practices in light of the Commissioner's findings. We have already taken strong measures to address the identified concerns with the deployment of our corporate information management system, CERRID, to be completed by October. Additionally, we are instituting measures to better document the rationales for our decision-making processes. Finally, in September, CSEC will launch an intensive awareness campaign for all staff, to promote more comprehensive measures to document our activities and to improve current business practices.	March-28-08	CIO		October-30-08	Completed	**March 2011**: CIO [redacted] has lead and provided IM awareness activities, literature and internal web communications that emphasize IM stewardship and collaboration practices in an enterprise-wide IM Awareness campaign. Awareness for the correct/efficient use of the Access Default feature in CERRID has been done to ensure the need-to-know principle is respected while sharing information to the greatest extent possible. The DGITS Activity Area created and implemented a procedure for staff for assigning Default Access permissions to their documents in CERRID (RDIMS). See CERRID document 79686. Regular CERRID training courses include user selection of Access Defaults for each student based on their activity area and role; IM best practices for documenting daily work, activities and decisions; balancing need-to-know vs. collaboration and sharing of information.

44	Support to CSIS	Report to the CSE Commissioner on CSE Support to CSIS, Phase 1: Mandate (a)	**Observation no. 1** Ministerial directives issued to CSE and dated June 19, 2001 preceded the passage of Part V.1 of the National Defence Act and should be reviewed to ensure they are in keeping with the mandated authorities articulated in the legislation.	CSEC agrees with the Commissioner and have committed to revisiting these three MDs by the end of the year.	January-16-08	PC	B	December-30-08	Overdue	B - May 2011: CSEC recognizes the importance of updating all authority instruments such that they are consistent with CSEC legislation. Given the delay in proceeding with anticipated amendments to CSEC legislation, the Chief, CSEC has directed that the pre-legislation MDs on Support to Lawful Access, Privacy and Accountability be updated to meet the Commissioner's observation (**#44**, observation 1). The MDs are being addressed in priority sequence, beginning with Support to Lawful Access as this MD was also subject to a specific Commissioner recommendation (#31, recommendation 1). CSEC has completed initial analysis of the Support to Lawful Access MD and has identified a number of potential revisions to update the MD in keeping with current CSEC legislation and to provide greater clarity on the nature of CSEC technical and operational assistance to federal law enforcement and security agencies. Similar analysis will be completed for the Privacy and Accountability MDs to identify any revisions required for consistency with legislation. This work will continue through 2011-2012 and it is anticipated that updated MDs will be submitted for ministerial signature before the end of the fiscal year. Sep 2011: B-group has no new information. **November 2012** The MD for Support to Law Enforcement and National Security Agencies was signed in November 2011. The Accountability and Privacy MDs have not yet been signed by the minister as CSEC waited for PING changes to come into effect. We expect them to be signed in fall 2012.
44	Support to CSIS	Report to the CSE Commissioner on CSE Support to CSIS, Phase 1: Mandate (a)	**Observation no. 2** CSE's failure to ensure that material provided by CSIS has been lawfully acquired would appear to be contrary to the stated objective and requirements of CSE Operational Policy OPS-4-2.3	**Tied to Recommendation 1.**	January-16-08	-	-	-	38899	Completed

44	Support to CSIS	Report to the CSE Commissioner on CSE Support to CSIS, Phase 1: Mandate (a)	**Observation no. 3** CSIS requests for information that may relate to a specific investigation or warranted activity under section 12 of the CSIS Act, such as [redacted] may be more appropriately made and dealt with under CSE's (c) mandate, as they are in fact being used by CSIS to further an authorized investigation being conducted by CSIS.	**Tied to Recommendation 2.** The Commissioner indicated in his letter that OCSEC has shared a discussion paper on the topic (a vs. c) with CSEC. CSEC has provided a response to this discussion paper and is awaiting a reply. in the meantime, CSEC will continue to conduct its activities in a manner consistent with the legal advice provided by the DoJ.	January-16-08	PC	D3	-	-	Completed
44	Support to CSIS	Report to the CSE Commissioner on CSE Support to CSIS, Phase 1: Mandate (a)	**Observation no.4** The foregoing supports the recommendation made in the review of the Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005, submitted to the Minister on January 2008, that CSE should re-examine and reassess the legislative authority used to conduct its contact chaining activities [redacted]	**Tied to Recommendation 2.** The Commissioner indicated in his letter that OCSEC has shared a discussion paper on the topic (a vs. c) with CSEC. CSEC has provided a response to this discussion paper and is awaiting a reply. in the meantime, CSEC will continue to conduct its activities in a manner consistent with the legal advice provided by the DoJ.	January-16-08	PC	D3	-	-	Completed

44	Support to CSIS	Report to the CSE Commissioner on CSE Support to CSIS, Phase 1: Mandate (a)	**Observation no. 7** CSE should consider amending the Request for Release of Suppressed Information form to ensure it is clear to all GoC clients requesting suppressed information, that Section G of the form must be fully completed regardless of whether any action is contemplated based on the suppressed information requested.	CSEC will review and update the terminology used in policies and procedures, in order to improve consistency, by September 2008. Additional management direction will be provided to address any potential gaps identified by the Commissioner	January-16-08	PC	D2	-	-	D2 - April 09: D2 Policy Analysts ensure that all GoC clients requesting suppressed information fully complete Section G. D2 is in the process of "webifying" its ident release and sanitization forms, which will involve converting the current forms done in Word/Word Perfect into a PDF format with smart capabilities i.e. users will enter required information via automated forms. Mandatory fields within the form will be clearly identified. Users will be prompted to complete all mandatory fields. If any mandatory information is missing, users will be redirected to complete missing field(s) prior to submission. This is a long term project, with many external dependencies (e.g. CIO, GC clients). Target date is end of calendar year.
43	Metadata	Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005	**Finding no. 4:** We understand that CSE is currently reviewing its contact chaining activities [redacted] and that CSE is re-drafting OPS-1-10 "to ensure that there is clarity in how contact chaining is to be done". OCSEC supports this review and will monitor developments.	**Tied to Recommendation 2.** CSEC is also working with its legal counsel to re-examine and re-assess the management direction regarding these contact chaining activities. Policy is being revised to clarify approval authorities for these activities and will be completed by July 2008. In addition, practices have been modified to better document the case-by-case rationales regarding the appropriateness of part (a) of the mandate for these activities.	January-09-08	-	-	July-30-08	0	0

43	Metadata	Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005	**Finding no 11:** OPS-1 does not include definitions of or any references to network analysis and prioritization or contact chaining, CSE's two [redacted] metadata activities. Also, OPS-1 has no reference to the two operational procedures (noted above) that deal with metadata. In addition, we verified that the most current version of OPS-1, dated December 2006, does not include any reference to OPS-1-10. Given that OPS-1-10 is still in draft, and that it is the only formal guidance available to CSE employees, the fulfilment of Criteria 4 remains weak. (For discussion of OPS-1-10, please see Annex C).		January-09-08	PC	D2	-	Completed	D2 - April 09: Completed - these issues were addressed in Amendment 5 to OPS-1 in December 2008 (which has been superseded by Amendment 6 effective 11 March 2009).
43	Metadata	Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005	**Finding no. 12:** The [redacted] and [redacted] operational procedures do not provide adequate guidance respecting [redacted] research or target development metadata activities.	CSEC agrees with the Commissioner and have committed to revisiting these three MDs by the end of the year.	January-09-08	PC	B	December-30-08	Completed	B - April 09: Is this one about operating procedures or MDs?
43	Metadata	Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005	**Finding no. 15:** We suggest that CSE consult GoC legislation and policies regarding corporate record keeping and information management and ensure that it is in compliance.	CSEC has already advised the Commissioner that it is implementing an electronic corporate records management system and has also improved its management of hard-copy files, especially those related to activities conducted under Ministerial Authorization. The plan is for the CSEC electronic information management system to be fully implemented by October 2008.	January-09-08	CIO		October-30-08	Completed	Please provide an update