

A-2011-150

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

JAN 4 / 2011  
CCM# 8163  
SECRET  
For Information

**MEMORANDUM TO THE MINISTER**

**LIBERATION TIGERS OF TAMIL EELAM (LTTE)**

**SUMMARY**

- The Service assesses that the Liberation Tigers of Tamil Eelam (LTTE) continues to pose a threat to the security of Canada

**BACKGROUND:**

The Liberation Tigers of Tamil Eelam (LTTE) have operated for decades with the goal of establishing a separate and sovereign Tamil state in Sri Lanka. In May 2009, Sri Lankan government forces defeated the LTTE militarily, resulting in migration of LTTE cadres from South and South East Asia to western nations with large Tamil diasporas.

The Sri Lankan community in Canada is estimated to number between 250,000 to 300,000, and are mostly concentrated in the greater Toronto area.

PROCESSED BY CBS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

With Canada's large population of ethnic Sri Lankan Tamils, existing network of LTTE front groups such as the World Tamil Movement (WTM) in Canada, the Service assesses that the LTTE continue to pose a threat to the security of Canada.

The Service remains vigilant to the potential for acts of violence directed against Sri Lankan community interests in Canada,

Our coordinated efforts are reflective of the whole of government strategy to deter illegal migration to Canada.



Richard B. Fadden

c.c.: Deputy Minister of Public Safety

c.c.: National Security Advisor to the Prime Minister

THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO MANDATORY EXEMPTION UNDER THE ACCESS TO INFORMATION ACT OR THE PRIVACY ACT. THE INFORMATION OR INTELLIGENCE MAY ALSO BE PROTECTED BY THE PROVISIONS OF SECTION 37(1) and 38(1) OF THE CANADA EVIDENCE ACT. THE INFORMATION OR INTELLIGENCE MUST NOT BE DISCLOSED OR USED AS EVIDENCE WITHOUT PRIOR CONSULTATION WITH THE CANADIAN SECURITY INTELLIGENCE SERVICE.

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM # 8305  
**SECRET**  
For Information

JAN 18 2011

**MEMORANDUM TO THE MINISTER**

**MEDIA ARTICLES CLAIMING 12 CANADIANS AT  
AL QAEDA TRAINING CAMP IN PAKISTAN**

**BACKGROUND:**

On 15 January, the Asia Times published an article entitled "Al-Qaeda (AQ) to unleash Western Jihadis." The article, subsequently reported upon in numerous Canadian media outlets, alleges that a group of twelve Canadian militants is receiving jihadi training in AQ camps in North Waziristan for terror attacks in Canada.

The article identifies six of the alleged Canadians as Jean Paul, Leman Langlois, James Richard, Otto Paul, Thomas Lnu, and Paul Gall. The group was reportedly recruited and led by an individual named Abu Shahid, a leader of the Egyptian Jihad al-Islami.

On 15 January, CTV interviewed one of the co-authors of the Asia Times article, Syed Saleem Shahzad, who stated that he obtained his information from a source located in North Waziristan associated with the AQ training camp. He stated that he had no further information related to the identities of the individuals.

Leman-Langlois recently co-authored a non-fiction book titled "Le Terrorisme et L'Antiterrorisme au Canada," with Jean-Paul Brodeur. In a CBC interview conducted on 16 January, Leman-Langlois denied any affiliation with AQ and surmised that the individual listed as "Jean Paul" was likely a reference to the book's now deceased co-author, Jean-Paul Brodeur.

PROCESSED BY CSIS UNDER THE  
 PROVISIONS OF THE PRIVACY ACT AND/OR  
 ACCESS TO INFORMATION ACT  
 REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
 SUR LA PROTECTION DES RENSEIGNEMENTS  
 PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
 À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
 PROVISIONS OF THE PRIVACY ACT AND/OR  
 ACCESS TO INFORMATION ACT  
 REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
 SUR LA PROTECTION DES RENSEIGNEMENTS  
 PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
 À L'INFORMATION



Richard B. Fadden

c.c.: Deputy Minister of Public Safety

c.c.: National Security Advisor to the Prime Minister

THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO MANDATORY EXEMPTION UNDER THE ACCESS TO INFORMATION ACT OR THE PRIVACY ACT. THE INFORMATION OR INTELLIGENCE MAY ALSO BE PROTECTED BY THE PROVISIONS OF SECTION 37(1) and 38(1) OF THE CANADA EVIDENCE ACT. THE INFORMATION OR INTELLIGENCE MUST NOT BE DISCLOSED OR USED AS EVIDENCE WITHOUT PRIOR CONSULTATION WITH THE CANADIAN SECURITY INTELLIGENCE SERVICE.



Director - Directeur

**SECRET**  
**For Decision**

JAN 25 2011

**MEMORANDUM TO THE MINISTER**

**DELEGATION OF AUTHORITY - TREASURY BOARD DIRECTIVE ON  
THE MANAGEMENT OF EXPENDITURES ON TRAVEL,  
HOSPITALITY & CONFERENCES**

Given the nature of the Service's mandate, the organization needs to liaise continuously with both foreign allies and non-federal domestic partners. In order to ensure the continued efficient conduct of Service operations and in accordance with provisions of the new Treasury Board Directive on the Management of Expenditures on Travel, Hospitality and Conferences, I am requesting that you delegate the following authorities to the position of Deputy Head, Canadian Security Intelligence Service (CSIS):

- Approve alcoholic beverages, as provided for in the Directive;
- Approve hospitality costs over \$5,000 for events where the Service has a government-wide responsibility for a program, as provided for in the Directive. More specifically, for events involving departments and agencies from the Security and Intelligence (S&I) Community which may occasionally include representatives from academia and other allied or foreign intelligence agencies.

In addition, the Service also hosts, on a rotating basis,

SECRET

- 2 -

These events offer the opportunity to share and learn about issues of mutual concern in ways that would otherwise not be possible. In that light, I request that you give consideration to delegating to the Deputy Head, CSIS, the authority to:

- Approve hospitality costs over \$5,000 for events involving .

The delegation of this authority will require further discussion and approval from TBS.

I would be pleased to provide additional information to you or your staff should it be required.



Richard B. Fadden

- I agree
- I disagree

The Hon. Vic Toews, P.C., M.P.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.



Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM # 7914  
**CONFIDENTIAL**  
For Information

FEB - 1 2011

**MEMORANDUM TO THE MINISTER**

**CSIS PUBLIC REPORT 2009-2010**

**SUMMARY**

- The CSIS 2009-10 Public Report highlights the general threat environment, including international terrorism, domestic radicalization and extremism, foreign espionage and interference, and other threats such as weapons proliferation and cybersecurity.
- Overall, the report is consistent with past reports but may draw attention to foreign interference issues and overseas operations.
- The report is expected to be tabled in early February.

**BACKGROUND:**

The purpose of this briefing note is to provide you with a strategic overview of the Canadian Security Intelligence Service's (CSIS) 2009-2010 Public Report. CSIS will work with your office and the department to facilitate its tabling in Parliament, its distribution, and responses to any questions and inquiries from the media and public. There is no date confirmed, but I hope that the report will be tabled in early February.

I would also draw your attention to several items of greater potential, public interest.

First, the report notes that terrorism continues to be Canada's top security threat, and that domestic radicalization is of ever increasing concern. I would expect media commentary on this issue, especially given recent court cases, such as the "Toronto 18", and the successful Operation Samosa in Ottawa. Second, commentary on foreign interference, while consistent with past comments and reports, will likely garner media attention given recent controversy. Third, the Security Intelligence Review Committee's recent Annual Report highlighted the need for greater public discussion on Canada's foreign intelligence capabilities and needs. The CSIS Public Report also notes the Service's increasing foreign intelligence capabilities. Reporting could note a perceived confluence of these issues. Finally, the Business Modernization Project (BMP) was completed this year and led to significant organizational changes within the Service. As the BMP was previously unreported, intelligence stakeholders may take notice of the BMP and its relation to organizational effectiveness.

#### **DISCUSSION:**

The following provides a brief description of some of the key elements of our public report.

***Internationally Based Terrorism:*** Radical Islamist terrorism remains the greatest security threat to Canadians, both domestically and internationally. Internationally, Al Qaeda (AQ) and AQ affiliates are of most concern. The report notes that AQ and AQ affiliates are amorphous, quick to adapt, and will continue to pose significant security risks to Canada for the foreseeable future. Canada remains the only country specifically targeted by AQ senior leadership which has not yet been attacked.

***Domestic Radicalization:*** The report notes that domestic Islamist radicalization is of mounting concern. The recent convictions of several members of the Toronto 18, and other operations have put the issue squarely in the public spotlight. "Home-grown terrorists" have no known profile, coming from all ages and educational backgrounds, and can appear fully integrated into society, making detection and intervention more difficult.

***Foreign Espionage and Interference:*** Foreign espionage and interference continue to be strong priorities for CSIS and are particularly noteworthy given recent media reporting on the subject. The report notes that a number of foreign governments continue to covertly gather political, economic, and military information in Canada. It also states that a noticeable increase in economic espionage is posing risks to our control over strategic and critical infrastructure, and refers to ongoing efforts by some countries to illegally acquire and transfer technology from Canada, especially as it relates to weapons proliferation.

The report also notes that Canada has traditionally been vulnerable to foreign interference activities, and that foreign powers have used and intimidated Canada's diverse communities to pursue their own agendas, often linked to a "homeland conflict."

*Weapons of Mass Destruction:* The nexus of technological development and globalization continue to pose security challenges. North Korea and Iran's development of nuclear arms and potential proliferation are of continual concern to Canada and the international community, especially proliferation to non-state actors and terrorists.

*Cybersecurity:* Similarly, the global reach and reliance on the internet for almost all areas of our lives, pose significant security challenges. Networks are vulnerable to hacking, espionage, and potential shut-down. As Canada is one of the most technologically advanced countries in the world, we remain especially vulnerable to cyber threats and attacks.

*Security Screening:* The report notes that, over the past year, the number of individuals screened under the Service's government screening program more than doubled (from 137,400 to 323,040 assessments) because of the requirements from the 2010 Winter Olympics. The Service also saw an increase in the number of individuals screened under its immigration screening program (from 329,100 to 344,400 assessments).

*Domestic and International Cooperation:* CSIS cooperates regularly with law enforcement partners and various government agencies throughout Canada. The report notes that as threats have become more global, CSIS has increased its capacity to collect quality intelligence abroad, and that as of March 2010, CSIS had 280 foreign arrangements with intelligence organizations in 148 countries. The report also speaks to the Service's efforts to ensure that its cooperation with foreign partners is consistent with Canada's human rights obligations.

*Inside CSIS:* CSIS continues to be one of the most diverse organizations in Canada with near equal gender representation, and a strongly bilingual workforce (67%). The report further notes that nearly 30% of CSIS employees speak a language other than English or French. Like most organizations, CSIS faces recruitment and retention challenges due to increasing retirements, however, the Service believes that it is well placed to face these challenges with a strong brand that again this year made the list of Canada's "Top 100 Employers."

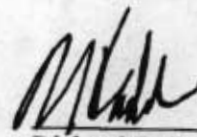
*Review and Accountability:* The report notes that CSIS is one of the most reviewed intelligence organizations in the world, subject to scrutiny of the Security and Intelligence Review Committee (SIRC), the Inspector General of CSIS, the Federal Court, and various officers of Parliament, such as the Privacy Commissioner and the Auditor General.

*Internal Reform:* CSIS has pursued some important internal reform measures through its recent Business Modernization Project (BMP). The most notable result is a new organizational structure, which aims to increase operational capacity, consolidate and enhance intelligence analysis, and increase corporate support.

*Public Communications:* CSIS' public profile remains high, with over 2,600 media reports this year alone. Although public communications will always be a challenge given the nature of the Service's mandate, CSIS has continued, where and when possible, to keep Canadians reasonably informed of its role in protecting national security by responding to a range of media, public, and

parliamentary inquiries in an unclassified manner, and by participating in community outreach programs.

CSIS has also continued its successful Academic Outreach Program (AOP), which provides our personnel with access to leading expertise to help refine our understanding of current and emerging security issues. The AOP provides an arena to share insights on issues and developments relating to the Service's mandate, and to provide a better understanding within the community of the government's intelligence priorities.



Richard B. Fadden

- c.c.: Deputy Minister of Public Safety
- c.c.: National Security Advisor to the Prime Minister

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM # 8350  
**SECRET**  
For Information

FEB - 1 2011

**MEMORANDUM TO THE MINISTER**

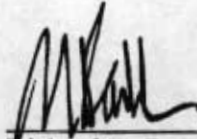
**VANDALISM AT MONTREAL-AREA SYNAGOGUES AND JEWISH SCHOOL**

**BACKGROUND:**

Articles in the *Montreal Gazette* and *Jerusalem Post* of 17 January 2011 reported on a series of attacks the night before on several Montreal-area synagogues and a Jewish school. The *Jerusalem Post* cited the chief of security of the Montreal Jewish community, Rabbi Reuben Poupko, who complained that until now such events "haven't garnered any attention," adding that "it's increasing in intensity and frequency. These are not just crimes against buildings. They're crimes against a community".

In all, four synagogues and one Jewish school were vandalized on 16 January 2011. At each location the vandalism involved windows broken by rocks.

PROCESSED BY CNS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.



Richard B. Fadden

c.c.: Deputy Minister of Public Safety

c.c.: National Security Advisor to the Prime Minister

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO MANDATORY EXEMPTION UNDER THE ACCESS TO INFORMATION ACT OR THE PRIVACY ACT. THE INFORMATION OR INTELLIGENCE MAY ALSO BE PROTECTED BY THE PROVISIONS OF SECTION 37(1) and 38(1) OF THE CANADA EVIDENCE ACT. THE INFORMATION OR INTELLIGENCE MUST NOT BE DISCLOSED OR USED AS EVIDENCE WITHOUT PRIOR CONSULTATION WITH THE CANADIAN SECURITY INTELLIGENCE SERVICE.



Director - Directeur

**SECRET**  
**For Decision**  
FEB - 3 2011

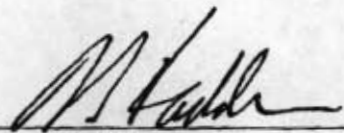
**MEMORANDUM TO THE MINISTER**

**DELEGATION OF AUTHORITY - TREASURY BOARD DIRECTIVE ON THE  
MANAGEMENT OF EXPENDITURES ON TRAVEL, HOSPITALITY &  
CONFERENCES**

Given the nature of the Service's mandate, the organization needs to liaise continuously with both foreign allies and non-federal domestic partners. In order to ensure the continued efficient conduct of Service operations and in accordance with provisions of the new Treasury Board Directive on the Management of Expenditures on Travel, Hospitality and Conferences, I am requesting that you delegate the following authority to the position of Deputy Head, Canadian Security Intelligence Service (CSIS):

- Approve alcoholic beverages, as provided for in the Directive.

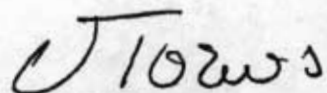
I would be pleased to provide additional information to you or your staff should it be required.

  
Richard B. Fadden

CSIS / SCRS  
160  
FEB 08 2011

- I agree  
 I disagree

DIR

  
The Hon. Vic Toews, P.C., M.P.

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

**SECRET**  
**CCM# 8447**  
**For Information**

**MEMORANDUM TO THE MINISTER**

**THE TOMMY DOUGLAS FILE AND RECENT COURT ACTIVITIES**

**BACKGROUND:**

Further to my note of 31 March 2010, the Service continues to be involved in proceedings to withhold certain information contained in the Tommy Douglas file from public disclosure. Originally requested under the *Access to Information Act (ATIA)*, the matter is now before the Federal Court as the applicant was dissatisfied with the CSIS recommendation to the Library and Archives of Canada (LAC) to withhold information, LAC's agreement, and the Information Commissioner's support thereof.

In an *in camera ex parte* hearing convened on 30 November 2010,

the Service recommended to LAC that it disclose further information, withholding only that which is of would tend to identify human sources. The information recommended for release – some of which will elicit media interest – will be filed with the Court, likely on 10 February, at which point they will become public. A public hearing into the matter will take place on 23 February.



**DISCUSSION:**

As part of the additional disclosure, CSIS has recommended the release of all information emanating from technical intercepts where the investigation to which it related has been terminated for a significant number of years, including those directed against such groups as the Voice of Women, the Communist Party of Canada, and the Labour Progressive Party. The disclosure will also include information about the former RCMP Security Service's general operational interest and investigations of possible subversive activities occurring within the Parliamentary precinct. Indeed, the documents contain reporting on the activities of some former Cabinet Ministers, Members of Parliament, their staff, and groups and individuals who have sought their assistance on a number of matters.

Releasing information of this nature represents a departure from the manner in which requests for historical records have been processed by CSIS under the *ATIA*.

If this information were disclosed, the identities of human sources  
could be compromised.

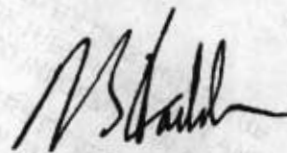
It should be noted that the Service's review is based on national security considerations only and that the documents, in fact, belong to LAC, not the Service. As the original *ATIA* request was made to LAC, the decision and discretion is theirs to apply any personal information exemptions related to individuals mentioned in the Tommy Douglas file.

**CONSIDERATIONS:**

The public release of this information, although likely to attract considerable media attention,

CSIS expects that this release, and the subsequent public hearing into the matter, is going to attract a significant amount of media attention. While the vast majority of the information regarding Tommy Douglas' activities has already been released, this further release will disclose, for the first time, some of his private communications with and links to other Parliamentarians.

CSIS Communications Branch is working closely with counterparts at Public Safety Canada, Canadian Heritage, and Library and Archives Canada to ensure that a comprehensive communications strategy is in place.



Richard B. Fadden

d/c.: National Security Advisor to the Prime Minister  
c.c.: Deputy Minister of Public Safety

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO MANDATORY EXEMPTION UNDER THE ACCESS TO INFORMATION ACT OR THE PRIVACY ACT. THE INFORMATION OR INTELLIGENCE MAY ALSO BE PROTECTED BY THE PROVISIONS OF SECTION 37(1) and 38(1) OF THE CANADA EVIDENCE ACT. THE INFORMATION OR INTELLIGENCE MUST NOT BE DISCLOSED OR USED AS EVIDENCE WITHOUT PRIOR CONSULTATION WITH THE CSIS

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

**BY HAND**

**SECRET**

MAY 26 2011

The Honourable Vic Toews, P.C., Q.C., M.P.  
Minister of Public Safety

Dear Minister:

The following is to provide you with an update on the status of the Service's  
*CSIS Act* Section 17(1)(b) foreign arrangement with

The Service's foreign arrangement with [redacted] was approved in [redacted]  
with a caveat that CSIS provide you with an update [redacted] following its  
implementation.

Liaison and exchanges between our organizations are primarily  
managed via the Service's

[redacted] maintains regular contact with  
representatives of the

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

.../2

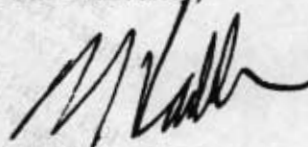
PROCESSED BY CRIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND  
ACCÈS À L'INFORMATION ACT  
REVISÉ PAR LE SGRS EN VERTU DE LA  
LOI SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET DE LA LOI SUR L'ACCÈS À L'INFORMATION

It is the Service's assessment that this arrangement continues to be productive and remains essential to our security intelligence collection requirements in the region linked to the security of Canada, its interests and its allies. is currently the only organization with some capacity to provide key intelligence on security threats emanating from that country,

Recognizing the current situation the Service is managing this relationship cautiously and effectively, and I am confident that our exchanges with the will contribute to the protection of Canada and its interests, while adhering to Canada's foreign policy

As per a Ministerial caveat, CSIS will continue to assess and review its cooperation with the on an ongoing basis and will seek your authorization to renew this foreign arrangement in a period of

Yours sincerely,



Richard B. Fadden

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
TRAITÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION



Director - Directeur

**CLASSIFICATION:** Secret  
**FILE #:**  
**For Decision**

JUN - 1 2011

**MEMORANDUM TO THE MINISTER**

**ESTABLISHMENT OF A CSIS ACT s.17(1)(b) FOREIGN ARRANGEMENT WITH**

**SUMMARY**

- In accordance with the Ministerial Direction on Foreign Arrangements and Cooperation, and pursuant to Section 17(1)(b) of the *CSIS Act*, your authorization is requested to establish a foreign arrangement between the Canadian Security Intelligence Service (CSIS) and

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR  
L'ACCÈS À L'INFORMATION

The Service's discussions with the ' were deemed positive and the latter demonstrated an interest in exchanging information with CSIS on issues of mutual interest, including those linked to international counter terrorism efforts.

.../2

**CLASSIFICATION: Secret**  
**FILE #:**

Based on the results of these discussions, the Service is requesting authorization to establish a s.17(1)(b) foreign arrangement with the

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

CSIS has an established s.17(1)(b) foreign arrangement with

It is assessed that an arrangement with the \_\_\_\_\_ would not adversely impact the Service's existing arrangements with these partners.

The Service is not aware of information indicating issues of corruption or human rights violations committed specifically by the \_\_\_\_\_. A review of open-source reporting from various human rights organizations yielded no evidence of allegations of human rights abuses committed by the \_\_\_\_\_.

The Service's posture regarding any exchanges with the \_\_\_\_\_ would respect all corresponding caveats and Ministerial directives on exchanges with foreign agencies, and would remain consistent with the Canadian government's foreign policy objectives.



Richard B. Fadden

- I agree
- I disagree

\_\_\_\_\_  
The Hon. Vic Toews, P.C., M.P.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION



Canadian Security  
Intelligence Service



Director - Directeur

Service canadien du  
renseignement de sécurité

**CLASSIFICATION:** Secret  
**FILE #:**  
**For Information**

JUN - 2 2011

**MEMORANDUM TO THE MINISTER**

**SUSPENSION OF FOREIGN ARRANGEMENT WITH**

In accordance with the Ministerial Directive on Foreign Arrangements and Cooperation, I am writing to inform you of the Canadian Security Intelligence Service's decision to suspend its existing *CSIS Act* Section 17(1)(b) foreign arrangement with

The Service's Ministerially-approved foreign arrangement with the originally established

Liaison and exchanges between  
CSIS and the are primarily managed via the CSIS

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISE PAR LE SCRS EN VERTUE DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCES  
A L'INFORMATION.

.../2

**CLASSIFICATION: Secret**  
**FILE #:**  
**For Information**

The Service will continue to closely monitor developments in order to assess their impact on the and the Service's existing foreign arrangement with same, CSIS will only consider lifting this self-imposed suspension and re-activate the arrangement when the situation



Richard B. Fadden

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION



Director - Directeur

JUN - 3 2011

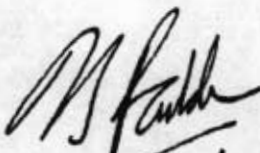
**MEMORANDUM TO THE MINISTER**

**ACCESS TO INFORMATION AND PRIVACY ANNUAL REPORTS**

I have the pleasure of enclosing the Canadian Security Intelligence Service (CSIS) Access to Information and Privacy Annual Reports for the reporting period of April 1, 2010 to March 31, 2011, for tabling in the House of Commons.

In compliance with the instructions outlined by the Treasury Board Secretariat (TBS), the reports are separate and distinct, they contain general statistics on the administration of the Acts, including the number of requests received and processed by the Service, along with summaries of the number of complaints made to the Privacy and Information Commissioners of Canada. Over and above the TBS reporting requirements, the Service has included multi year comparison statistical trends on the administration of both Acts.

The reports are positive and do not contain any significant issues. The 2010-2011 statistical data on the administration of the *Access to Information Act* depicts a high compliancy on-time completion rate of 97%. Similarly, our on-time completion rate under the *Privacy Act* is 99%.

  
Richard B. Fadden

Encl.

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM # 9360  
**SECRET**  
For information  
JUN 15 2011

**MEMORANDUM TO THE MINISTER**

**CSIS RELATIONSHIP WITH**

**SUMMARY**

- While CSIS continues to closely scrutinize its relations with iaison  
with these agencies remains crucial to Canada's national security interests

**BACKGROUND:**

DISCUSSION:

The Service's s.17 arrangement with  
intelligence with

CSIS selectively shares

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
TRAITÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
TRAITÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
TRAITÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

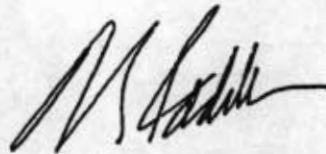
**ASSESSMENT:**

CSIS arrangements with \_\_\_\_\_ established in accordance with s.17 of the *CSIS Act*, remain crucial to the Service's ability to properly advise Government on threats to the security of Canada emanating from the region. \_\_\_\_\_ it is the Service's assessment that they continue to be productive and essential to our intelligence collection requirements. The Service continues to obtain valuable intelligence on threats to Canadian interests as a result of its efforts to develop contacts \_\_\_\_\_ - cooperation that would simply not be possible without active engagement.

I wish to assure you that CSIS approaches \_\_\_\_\_

Service's posture regarding any exchanges with the \_\_\_\_\_ will continue to respect Ministerial direction on exchanges with foreign agencies, and remain consistent with the Government of Canada's foreign policy objectives.

The



Richard B. Fadden

- c.c.: National Security Advisor
- c.c.: Deputy Minister of Public Safety

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM # 9473  
**SECRET**  
For Decision

**MEMORANDUM TO THE MINISTER**

**CSIS ACT S. 17 ARRANGEMENT WITH THE**

**BACKGROUND :**

The *Canadian Security Intelligence Service Act (CSIS Act)* requires that I seek your approval to enter into arrangements on cooperation with domestic and foreign agencies. Thus, pursuant to sub-paragraph 17(1)(a)(i) of the *CSIS Act*, I am seeking your approval to enter into a framework arrangement on cooperation with

**DISCUSSION :**

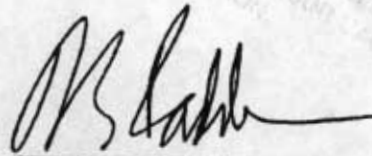
The framework arrangement will set out the terms and conditions of our cooperation. As well, it will layout the nature and scope of working agreements to implement the cooperation between the two organizations. The Memorandum of Understanding (MOU) will confirm the foundation of our cooperation for the purpose of information and intelligence collection, intelligence sharing and operational support in accordance with relevant legal authorities. It will also layout the general principles of the administration and management of such activities. Furthermore, the arrangement will outline our respective responsibilities in regard to the use and safeguarding of shared information

This MOU with \_\_\_\_\_ is also intended to be the vehicle that will enable the two organizations to review existing agreements and with a view to merge their content where applicable.

**CONCLUSION :**

The framework arrangement is attached for your review. Annex A of this document is provided to exemplify the type of working agreements which will be negotiated to implement the arrangement.

I am available to discuss this matter with you if you wish.



Richard B. Fadden

- I agree / approve
- I disagree / disapprove

The Hon. Vic Toews, P.C., Q.C., M.P.

Enclosure: 1

c.c. : Deputy Minister of Public Safety

This document constitutes a records which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be projected by the provisions of section 37(1) and 38(1) of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with CSIS.





Director - Directeur

CCM # 9476  
TOP SECRET  
For Information

JUL 12 2011

**MEMORANDUM TO THE MINISTER OF PUBLIC SAFETY**

**COURT DECISION ON THE ALMALKI,  
ELMAATI AND NUREDDIN SECTION 38 CANADA EVIDENCE ACT CASE**

- The 13 June Federal Court of Appeal decision in the Almalki, Elmaati and Nureddin section 38 *Canada Evidence Act* case allowed the Attorney General's appeal to protect information previously ordered disclosed. The Court of Appeal also decided that CSIS human sources do not receive absolute protection under the informer privilege rule.
- The Crown will not appeal the decision regarding human source protection.

**BACKGROUND:**

On 13 June 2011, the Federal Court of Appeal issued a decision in the Almalki, Elmaati and Nureddin section 38 *Canada Evidence Act (CEA)* case regarding a decision of the Federal Court to disclose information in relation to civil lawsuits commenced by these three individuals in the Ontario Superior Court of Justice.

The lower court ordered the disclosure of the information because it believed, pursuant to section 38 of the *CEA*, that the public interest in the disclosure of the information outweighed the public

interest in non-disclosure. In response, the Attorney General filed an appeal with the Federal Court of Appeal on the grounds that the disclosures would be injurious to Canada's international relations or national security. The Federal Court of Appeal allowed the appeal.

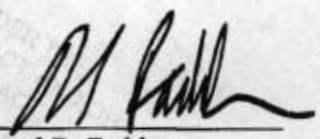
Instead, the Court decided that a case-by-case application of a public interest balancing test under s.38 of the *CEA*, as undertaken by the lower court, is required and that this approach expresses the intent of Parliament.

With respect to this part of the decision, the Court noted that, while sections 18 and 19 of the *CSIS Act* provide for the protection of the identity of confidential sources, it also allows for exceptions where disclosure is required by law. This, the Court stated, demonstrated Parliament's intention that this protection not be absolute like the informer privilege. Through a reference to a Supreme Court of Canada decision regarding the creation of class privileges, the Court noted that any future class privilege for CSIS human sources would likely only be created through legislative action in order to address the full scope of potential legal, political and social impact.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
TRAITEMENT PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
TRAITEMENT PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION



Richard B. Fadden

- c.c.: National Security Advisor to the Prime Minister
- c.c.: Deputy Minister of Public Safety

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
TRAITEMENT PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO MANDATORY EXEMPTION UNDER THE ACCESS TO INFORMATION ACT OR THE PRIVACY ACT. THE INFORMATION OR INTELLIGENCE MAY ALSO BE PROTECTED BY THE PROVISIONS OF SECTION 37(1) and 38(1) OF THE CANADA EVIDENCE ACT. THE INFORMATION OR INTELLIGENCE MUST NOT BE DISCLOSED OR USED AS EVIDENCE WITHOUT PRIOR CONSULTATION WITH THE CANADIAN SECURITY INTELLIGENCE SERVICE.

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM # : 11-0003

**SECRET**

**For Decision**

AUG 03 2011

**MEMORANDUM TO THE MINISTER**

**CSIS ACT S.17 ARRANGEMENT**  
**WITH**

The *Canadian Security Intelligence Service Act (CSIS Act)* requires that I seek your approval to enter into arrangements on cooperation with domestic and foreign agencies. Thus, pursuant to sub-paragraph 17(1)(a)(i) of the *CSIS Act*, I am seeking your approval to enter into an arrangement with

**BACKGROUND:**

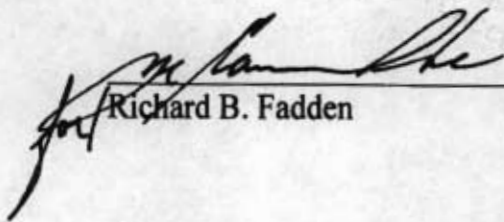
The establishment of this agreement sets out the process for

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTUE DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

**CONCLUSION:**

A draft of the arrangement is attached for your review. Annex A of this draft is provided to exemplify the type of working form necessary to implement the arrangement.

I am available to discuss this matter with you if you wish.

  
Richard B. Fadden

- I agree / approve
- I disagree / disapprove

The Hon. Vic Toews, P.C., Q.C., M.P.

cc : Deputy Minister, Public Safety

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be projected by the provisions of section 37(1) and 38(1) of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with CSIS.



Director - Directeur

**CLASSIFICATION: Secret**  
**FILE #: 205-26**  
**For Decision**

AUG 03 2011

**MEMORANDUM TO THE MINISTER**

**ESTABLISHMENT OF A CSIS ACT s.17(1)(b) FOREIGN ARRANGEMENT WITH**

**SUMMARY**

- In accordance with the Ministerial Direction on Foreign Arrangements and Cooperation, pursuant to Section 17(1)(b) of the *CSIS Act*, your authorization is requested to establish a foreign arrangement between the Canadian Security Intelligence Service (CSIS) and

The Service is requesting authorization to establish a s.17(1)(b) foreign arrangement with

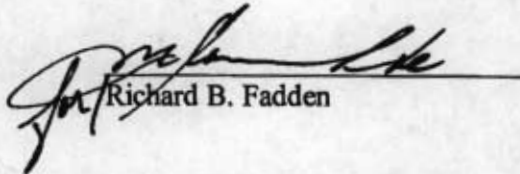
.../2

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

The Service's posture regarding cooperation with the \_\_\_\_\_ would respect all corresponding caveats and Ministerial directives on exchanges with foreign agencies, and would remain consistent with the Canadian government's foreign policy objectives.

  
Richard B. Fadden

- I agree
- I disagree

\_\_\_\_\_  
The Hon. Vic Toews, P.C., M.P.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.



Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM # 9587  
PROTECTED A  
For Decision

**MEMORANDUM TO THE MINISTER OF PUBLIC SAFETY**

**UPDATES TO THE CSIS ACCESS TO INFORMATION AND PRIVACY (ATIP)  
DELEGATION ORDERS**

**BACKGROUND :**

You will find enclosed updated versions of the Service's Delegation Orders covering the administration of the *Access to Information Act and Privacy Act* (the "Acts"). These Orders authorize individuals occupying designated positions in the Service to exercise, on behalf of the head of the institution, their powers, duties or functions under the *Acts*.

The last Delegation Orders were issued by you on 26 February 2010. In spite of the fact that they are fairly recent, the Delegation Orders require updating. The titles of various officials have changed as a result of a realignment of the Service's Secretariat, and we are seeking additional delegated authority under the *Privacy Act* for the Deputy Chief and Unit Heads.

**DISCUSSION :**

Currently, all records processed by the Service are reviewed and signed off by the Chief ATIP. Last year, the Chief ATIP reviewed an upwards of 97,000 pages. These figures are not expected to diminish in the foreseeable future. The substantial increases in ATIP requests have made it unfeasible to maintain the status quo. The sheer volume of the material to be reviewed has made it impossible for one person to carry. Given the lower risk associated with privacy disclosures, it is suggested that the *Privacy Act* Delegation Order be expanded to include the Deputy Chief and Unit Heads. This measure would divert the review of thousand of pages. The devolution of these powers would allow the Chief ATIP to devote greater attention to requests made under the *Access to Information Act*. Greater efficiencies and improved response times would be gained. You have already approved a similar delegation scheme for the RCMP, CBSA and CSC.

Full delegated authority is requested from the Director to Unit Heads under the *Privacy Act*. The revised Privacy Order corrects the previous one which should have included section 8(2) in its entirety and section 20 of the *Act*. Section 8(2) contains the 'public interest' override which, as a

matter of course, must be considered in every case where an institution applies the personal information exemption. Hence, officials who are listed on the Delegation Order must be empowered to apply the section in order to undertake the balancing test that needs to be applied. It goes without saying that any formal release of personal information 'in the public interest' would be brought to my attention for consideration and approval. Section 20 is the exemption to protect federal-provincial relations which can only be applied after consultation with the Privy Council Office. We see no issue in requesting this additional authority as the exemption can only be applied after consultation with the Privy Council Office.

The *Access to Information Act* Delegation Order remains essentially the same, with the exception of the authority for the Director General Litigation and Chief ATIP to exempt information pursuant to section 14 (the federal-provincial relations exemption). Once again, we see no issue as the exemption can only be applied after consultation with the Privy Council Office, and we do not understand why it was not included in the original Order.

As an aside, the number of complaints to the Information Commissioner have risen and it is expected that matters brought to the Courts will also rise. Having the proper delegated authority in place will avoid potential jeopardy to Service assets, when exemption decisions are challenged.

**RECOMMENDATION:**

That you approve the request for additional delegated authority under both *Acts*. If you agree, new Orders are enclosed at Tab 1 for your signature. The current Orders are enclosed at Tab 2.



Richard B. Fadden

- I agree / approve
- I disagree / disapprove

The Hon. Vic Toews, P.C., Q.C., M.P.

Enclosures: 2

c.c. : Deputy Minister of Public Safety

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM # 9689  
**CONFIDENTIAL**  
For Decision

AUG 11 2011

**MEMORANDUM TO THE MINISTER**

**CSIS ACT S.17 ARRANGEMENT WITH  
PUBLIC WORKS GOVERNMENT SERVICES CANADA**

**BACKGROUND :**

The *Canadian Security Intelligence Service Act (CSIS Act)* requires that I seek your approval to enter into arrangements on cooperation with domestic and foreign agencies. Thus, pursuant to sub-paragraph 17(1)(a)(i) of the *CSIS Act*, I am seeking your approval to enter into an arrangement on cooperation with Public Works Government Services Canada (PWGSC) regarding International Traffic in Arms Regulations (ITAR).

**DISCUSSION :**

ITAR is a set of US Government regulations covering the export and import of defence-related articles. Until recently, ITAR proscribed the transfer of defence-related articles to dual and third country nationals employed in the Canadian defence and aerospace industries, a rule that imposed significant legal challenges for Canadian employers.

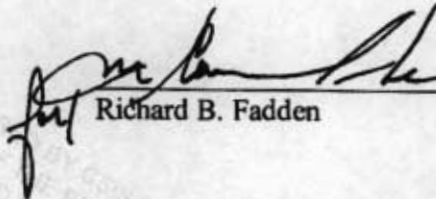
On May 16, 2011, the US Government amended its ITAR rules to allow companies to vet their employees to ensure that they do not pose a proliferation risk. Under the new amendment PWGSC's Controlled Goods Directorate (CGD) will ensure a certain standard of vetting as part of its "Enhanced Security Strategy." If the CGD determines that an individual is of possible proliferation concern, it intends to request indices checks from CSIS and other agencies such as the RCMP and CBSA.

The new ITAR rule comes into effect on August 15, 2011, and the Service is ready to sign an MOU with PWGSC.

**CONCLUSION :**

I am writing to seek your approval, under s.17 of the *CSIS Act*, to enter into an arrangement with PWGSC to allow the Service to provide support to PWGSC by vetting individuals of possible proliferation concern who have access to controlled goods. The arrangement is attached for your review.

I am available to discuss this matter with you if you wish.



Richard B. Fadden

- I agree / approve
- I disagree / disapprove

The Hon. Vic Toews, P.C., Q.C., M.P.

Enclosure: 1

This document constitutes a records which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be projected by the provisions of section 37(1) and 38(1) of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with CSIS.

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

AUG 23 2011

The Honourable Vic Toews, P.C., Q.,C., M.P.,  
Minister of Public Safety  
269 Laurier Avenue West  
Ottawa, Ontario.  
K1A 0P8

Dear Minister:

I am writing in response to the invitation to attend the Canadian Police and Peace Officers's Memorial Service which will be held on September 25<sup>th</sup>, 2011. I am pleased to be able to accept your invitation to attend both the ceremony and the reception.

Further, I confirm that the invitation has been extended to members of the Canadian Security Intelligence Service's (CSIS) Executive board, several of whom have the intent to attend.

My office will liaise with yours and/or Public Safety Canada officials in relation to CSIS representation at the event.

With appreciation for the invitation.

Sincerely,

Richard B. Fadden

*5. 11. 2011  
Mr. Toews*

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

CSIS / SCRS

AOUT 03 2011  
AUG 03 2011

Mr. Richard B. Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Ottawa, Ontario K1J 1B7

DIR

Dear Mr. Fadden:

The Canadian Police and Peace Officers' Memorial Service is an annual event which commemorates police and peace officers who have died in the line of duty and is of great importance to the policing community. This year marks the 34th annual memorial service, and will be held on Parliament Hill on Sunday, September 25, 2011.

I would like to take this opportunity to invite you and your senior staff to attend the Memorial Service and the reception following the service.

I look forward to seeing you there.

Yours sincerely,

*Vic Toews*

Vic Toews, P.C., Q.C., M.P.

*I will take to Mr.  
Mr. Fadden reply to Mr.  
each division  
R*

In addition to the Canadian Police and Peace Officers' Memorial Service, a number of weekend events have been arranged for those traveling to Ottawa.

## **2011 MEMORIAL WEEKEND EVENTS**

### **Thursday, September 22, 2011**

8:45 am National Peace Officers Memorial Run leaves Queen's Park, Toronto. For more information contact [natalie.hiltz@peelpolice.on.ca](mailto:natalie.hiltz@peelpolice.on.ca) or [www.npomr.org](http://www.npomr.org)

### **Friday, September 23, 2011**

5:00 pm - 9:00 pm Meet and greet, lasagne & salads \$10, *Russell's Lounge*, 141 Catherine Street  
8:00 pm - 2:00 am DJ & dancing at *Russell's Lounge* and live music in the tent.

### **Saturday, September 24, 2011**

#### **16<sup>th</sup> Annual Canadian Police Association Memorial Golf Tournament**

(For further information contact Michael Gendron at 613-231-4168 ext. 229) [www.cpa-acp.ca](http://www.cpa-acp.ca)



9:00 am - 3:00 pm 10<sup>th</sup> Annual Canadian Police Memorial Weekend Trade Show at Tom Brown Arena, 141 Bayview Road (proceeds to CHEO). Tickets \$2 at the door; \$10/table. For more information contact Bob Pyefinch at [pyefinch@sympatico.ca](mailto:pyefinch@sympatico.ca) or 613-345-8431.

10:00 am - 3:00 pm The Big Pull (Tug-of-War) Mooney's Bay Beach, Ottawa Police Association (proceeds to Ottawa Mission) [www.thebigpull.com](http://www.thebigpull.com)

1:00 pm - 3:00 pm Canadian Police Professional Solo Piping Contest. Piobaireachd (classical) component. Ottawa City Hall, 111 Lisgar St. Tickets \$10 at the door. (proceeds to CPA-Robert Warner Memorial Fund)

3:00 pm National Peace Officers Memorial Run arrives on Parliament Hill.  
Ride to Remember arrives on Parliament Hill.

4:00 pm - 8:00 pm Prime Rib Roast of beef with all trimmings \$15 at *Russell's Lounge*

7:00 pm - 9:00 pm Canadian Police Professional Piping Contest March and Strathspey component (licensed). Ottawa City Hall, 111 Lisgar St. Tickets \$10 at door. (proceeds to Memorial)

7:00 pm - 9:00 pm Choral Showcase (5 Chorus') Dominion-Chalmers United Church, 355 Cooper Street. Contact Bob Kruikemeijer 613-852-7557

8:00 pm - 2:00am Entertainment at *Russell's Lounge* with D.J. and live music in the tent

### **Sunday, September 25, 2011**

7:00 am - 10:00 am Memorial Service Breakfast at *Russell's Lounge*, sponsored by the Canadian Police Association

9:00 am - 9:55 am Reading of the entire Honour Roll of fallen officers at the Memorial Pavilion  
Parliament Hill, West Corner

9:00 am - 10:00 am Police/Peace Officer Parade form up, Supreme Court of Canada, Kent and Wellington

9:30 am - 10:30 am Seating for Memorial Service

9:45 am - 10:00 am Motorcycles proceed to Hill, East Drive

10:00 am - 10:15 am Prelude by police choirs

10:20 Parade Steps Off (Parade Orders at [www.thememorial.ca](http://www.thememorial.ca))

#### **11:00 am - 12:00 pm 34<sup>th</sup> Annual Memorial Service Parliament Hill (rain or shine)**



12:00 pm - 1:30 pm Reception in Centre Block hosted Public Safety Canada

12:30 pm - 3:00 pm Memorial Service Luncheon (build your own sandwich bar and hot chilli) \$10  
at *Russell's Lounge*

**SHUTTLE VANS TO MEMORIAL WEEKEND EVENTS ONLY: 613-952-4204 (Next of Kin)**  
**(Friday and Saturday 08:00 - 24:00, Sunday 06:30 - 16:00)**

**FOR MORE INFORMATION: 613-880-5221**

**FOR HOTEL INFORMATION: [www.ottawahotels.com](http://www.ottawahotels.com)**

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

JUL 28 2011

UNCLASSIFIED

Mr. Richard Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Gloucester, Ontario K1J 1B7

CSIS / SCRS

980  
AUG 23 2011

DIR

Dear Mr. Fadden,

I previously indicated to you that officials in Public Safety Canada were preparing more comprehensive guidance on the Canadian Security Intelligence Service's (CSIS) information sharing practices.

Please find attached my new direction to CSIS on "Information Sharing with Foreign Entities."

This Ministerial Direction replaces the direction issued in 2009 on "Information Sharing with Foreign Agencies," as well as a copy of my letter to you dated December 7, 2010.

Yours sincerely,

*V Toews*

Vic Toews, P.C., Q.C., M.P.

Enclosure

Canada



**Ministerial Direction to the Canadian Security Intelligence Service:  
Information Sharing With Foreign Entities<sup>1</sup>**

In the current threat environment, terrorism is the top national security priority of the Government of Canada. In this context, it is essential that the Canadian Security Intelligence Service (CSIS) is able to maintain strong relationships with foreign entities, and can share information with them on both a routine and an urgent basis. CSIS must also be able to quickly share information with other key domestic stakeholders, including federal departments and agencies that have the mandate and responsibility to respond to serious threats before they materialize.

The following Ministerial Direction provides guidance to the Director of CSIS, pursuant to section 6(2) of the *CSIS Act*, on information sharing with foreign entities.

**1. Canada's Legal Obligations**

Sharing information with foreign entities is an integral part of CSIS' mandate. It is also a formal obligation pursuant to Canada's adoption of various international resolutions and agreements.

The Government of Canada opposes in the strongest possible terms the mistreatment of any individual by any foreign entity for any purpose. The Government also has a duty to its own citizens and to its allies to prevent individuals engaging in threat related activities from causing harm, whether in Canada or in a foreign country.

The Government of Canada does not condone the use of torture or other unlawful methods in responding to terrorism and other threats to national security. The Government is committed to pursuing a principled and proportionate response to these threats, while promoting and upholding the values Canada seeks to protect.

Canada is a party to a number of international agreements that prohibit torture and other forms of cruel, inhuman, or degrading treatment or punishment. These include the *International Covenant on Civil and Political Rights* and the *Convention Against Torture and Other Cruel, Inhumane, or Degrading Treatment or Punishment (CAT)*. The *CAT* requires state parties to criminalize all instances of torture, and to take effective measures to prevent torture and other cruel, inhuman, or degrading treatment or punishment in any territory under their jurisdiction.

Torture is a criminal offence in Canada that has extraterritorial application. The *Criminal Code*'s provisions governing secondary liability also prohibit aiding and abetting the commission of torture, counselling the commission of torture whether or not the torture is committed, conspiracy to commit torture, attempting to commit torture, and being an accessory after the fact to torture.

<sup>1</sup> This Direction would not change existing legal authorities for sharing information with foreign entities. Although the term, foreign entity, has not been formally defined, it primarily refers to foreign government agencies and militaries. The term may also refer to military coalitions, alliances, and international organizations.

More broadly, section 7 of the *Canadian Charter of Rights and Freedoms* guarantees that "everyone has the right to life, liberty, and security of the person." Section 12 of the *Charter* prohibits "any cruel and unusual treatment or punishment," which Canadian courts have described as behaviour "so excessive as to outrage the standards of decency." This behaviour includes torture and other cruel, inhuman, or degrading treatment or punishment.

## 2. Definitions

"Mistreatment" means torture or other cruel, inhuman, or degrading treatment or punishment.

"Substantial risk" is a personal, present, and foreseeable risk of mistreatment.

- In order to be "substantial," the risk must be real and must be based on something more than mere theory or speculation.
- In most cases, the test of a substantial risk of mistreatment will be satisfied when it is more likely than not that there will be mistreatment. However, the "more likely than not" test should not be applied rigidly because in some cases, particularly where the risk is of severe harm, the "substantial risk" standard may be satisfied at a lower level of probability.

## 3. Information Sharing Principles

Sharing information with foreign entities is an integral part of CSIS' mandate. It is also a formal obligation pursuant to Canada's adoption of various international resolutions and agreements.

In sharing information, CSIS must act in a manner that complies with Canada's laws and legal obligations. It is to avoid any complicity in mistreatment by foreign entities.

CSIS must assess and mitigate potential risks of sharing information in ways that are consistent with its unique role and responsibilities.

CSIS must also assess the accuracy and reliability of information received, and properly characterize this information in any further dissemination. It must have in place reasonable and appropriate measures to identify information that is likely to have been derived from mistreatment.

The approval level that CSIS requires in order to share information must be proportionate to the risk of mistreatment that may result: the greater the risk, the more senior the level of approval required.

CSIS also has a responsibility to keep the Minister of Public Safety generally informed about its information sharing practices.

#### **4. Decision Making Process When There Is A Substantial Risk of Mistreatment In Sharing Information**

Except when there is a substantial risk, CSIS is responsible for establishing approval levels that are proportionate to the risks in sharing information with foreign entities. The following decision making process applies when there is a substantial risk of mistreatment of an individual.

When there is a substantial risk that sending information to, or soliciting information from, a foreign entity would result in the mistreatment of an individual, and it is unclear whether that risk can be mitigated through the use of caveats or assurances, the matter will be referred to the Director for decision.

In making his or her decision, the Director will normally consider the following information, all of which must be properly characterized in terms of its accuracy and reliability:

- the threat to Canada's national security or other interests, and the nature and imminence of that threat;
- the importance of sharing the information, having regard to Canada's national security or other interests;
- the status of the relationship with the foreign entity with which the information is to be shared, and an assessment of the human rights record of the foreign entity;
- the rationale for believing that there is a substantial risk that sharing the information would lead to the mistreatment of an individual;
- the proposed measures to mitigate the risk, and the likelihood that these measures will be successful (including, for example, the foreign entity's record in complying with past assurances, and the capacity of those government officials to fulfil the proposed assurance);
- the views of the Department of Foreign Affairs and International Trade (DFAIT); and
- the views of other departments and agencies, as appropriate, as well as any other relevant facts that may arise in the circumstances.

The Director may refer the decision whether or not to share information with the foreign entity to the Minister of Public Safety, in which case the Minister will be provided with the information described above.

The Director or Minister of Public Safety shall authorize the sharing of information with the foreign entity only in accordance with this Direction and with Canada's legal obligations.

#### **5. Use Of Information That May Have Been Derived Through Mistreatment By Foreign Entities**

As a general rule, CSIS is directed to not knowingly rely upon information derived through mistreatment by foreign entities.

In exceptional circumstances, CSIS may need to share the most complete information in its possession, including information from foreign entities that was likely derived through mistreatment, in order to mitigate a serious threat of loss of life, injury, or substantial damage or destruction of property before it materializes. In such rare circumstances, ignoring such information solely because of its source would represent an unacceptable risk to public safety.

When there is a serious risk of loss of life, injury, or substantial damage or destruction of property, CSIS will make the protection of life and property its priority. If CSIS needs to share information that was likely derived through mistreatment with appropriate authorities in order to mitigate a serious threat, the matter will be referred to the Director. All decisions shall be made only in accordance with this Direction and with Canada's legal obligations.

CSIS will take all reasonable measures to reduce the risk that any action on its part might promote or condone the use of mistreatment. Measures will also be taken to ensure that the information which may have been derived through mistreatment is accurately described, and that its reliability is properly characterized. Caveats will be imposed on information shared with both domestic and foreign recipients to restrict their use of information, as appropriate.

## 6. Support

To help ensure a consistent understanding of the risks of sharing information with foreign entities, DFAIT will continue to make its country human rights reports available to the intelligence and law enforcement community.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

**Instruction du ministre à l'intention du Service canadien du renseignement de sécurité sur l'échange d'information avec des organismes étrangers**<sup>1</sup>

Compte tenu des menaces actuelles, la lutte contre le terrorisme est la plus grande priorité du gouvernement du Canada en matière de sécurité nationale. Dans ce contexte, il est essentiel que le Service canadien du renseignement de sécurité (SCRS) puisse entretenir des relations solides avec les organismes étrangers et qu'il puisse échanger avec eux de l'information de manière courante ou urgente. Le SCRS doit également pouvoir échanger rapidement de l'information avec des intervenants clés au pays, y compris les ministères et organismes fédéraux qui ont pour mandat et responsabilité de combattre les menaces graves avant qu'elles ne se concrétisent.

La présente instruction du ministre, établit conformément au paragraphe 6(2) de la *Loi sur le SCRS*, apporte au directeur du SCRS des directives sur l'échange d'information avec des organismes étrangers.

### **1. Obligations juridiques du Canada**

L'échange d'information avec des organismes étrangers fait partie intégrante du mandat du SCRS. Il s'agit également d'une obligation découlant de l'adoption par le Canada de diverses résolutions et ententes internationales.

Le gouvernement du Canada s'oppose catégoriquement à ce que de mauvais traitements soient infligés à quiconque par un organisme étranger, quel que soit le but visé. Il a également le devoir envers ses citoyens et ses alliés d'empêcher les individus qui participent à des activités représentant une menace de causer du tort au Canada ou à l'étranger.

Le gouvernement du Canada s'oppose à l'utilisation de la torture et d'autres méthodes illicites pour combattre le terrorisme et les autres menaces à la sécurité nationale. Il est déterminé à recourir à une intervention proportionnelle et fondée sur des principes pour faire face aux menaces, tout en défendant les valeurs que le Canada cherche à protéger.

Le Canada est partie à un certain nombre d'ententes internationales qui interdisent la torture et les autres formes de peines et de traitements cruels, inhumains ou dégradants. Il est par exemple partie au *Pacte international relatif aux droits civils et politiques* et à la *Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants*. Cette convention exige que les États parties criminalisent toutes les formes de torture et prennent des mesures concrètes pour empêcher que des actes de torture ou que des peines ou des traitements cruels, inhumains ou dégradants soient infligés dans tout territoire relevant de leur compétence.

Au Canada, la torture est une infraction pénale de portée extraterritoriale. Les dispositions sur la responsabilité subsidiaire du *Code criminel* interdisent également aux personnes d'aider ou

<sup>1</sup> Le Cadre ne change rien aux obligations juridiques existantes en matière d'échange d'information avec des entités étrangères. Le terme entité étrangère, même s'il n'est pas défini de manière officielle, désigne d'abord et avant tout les organismes et services militaires étrangers. Il peut aussi s'appliquer à des coalitions militaires, des alliances et des organisations internationales.

d'encourager la commission d'un acte de torture, de conseiller la torture peu importe si un acte de torture est commis, de tenter ou de comploter de commettre un acte de torture ou d'être complice après le fait.

De façon plus générale, l'article 7 de la *Charte canadienne des droits et libertés* garantit que « chacun a droit à la vie, à la liberté et à la sécurité de sa personne ». L'article 12 de la Charte protège contre « tous traitements ou peines cruels et inusités », lesquels ont été définis par les tribunaux canadiens comme un comportement « excessif au point de ne pas être compatibles avec la dignité humaine », ce qui comprend la torture et les autres formes de peines ou de traitements cruels, inhumains ou dégradants.

## **2. Définitions**

« Mauvais traitement » s'entend de la torture ou de tout autre peine ou traitement cruel, inhumain ou dégradant.

« Risque substantiel » signifie qu'une personne court un risque personnel, actuel et prévisible de subir des mauvais traitements.

- Pour être « substantiel », le risque doit être réel et ne pas être uniquement théorique ou spéculatif.
- Dans la plupart des cas, l'existence d'un risque substantiel est établie s'il est « plus probable qu'improbable » que des mauvais traitements soient infligés à la personne. Cependant, ce critère ne doit pas être appliqué de manière absolue puisqu'il est possible dans certains cas d'établir l'existence d'un « risque substantiel » à un niveau de probabilité inférieure, surtout si une personne risque de subir un préjudice grave.

## **3. Principes liés à l'échange d'information**

L'échange d'information avec des organismes étrangers fait partie intégrante du mandat du SCRS. Il s'agit également d'une obligation découlant de l'adoption par le Canada de diverses résolutions et ententes internationales.

Lorsqu'il échange de l'information, le SCRS doit respecter les lois et les obligations juridiques du Canada. Il doit éviter également d'être complice de mauvais traitements infligés par des organismes étrangers.

Le SCRS doit évaluer et atténuer les risques qui pourraient être liés à l'échange d'information en tenant compte des responsabilités et rôles qui lui sont propres.

Le SCRS doit également évaluer l'exactitude et la fiabilité de l'information qu'il reçoit et qualifier adéquatement l'information avant de la transmettre à d'autres. Il doit avoir en place des mesures raisonnables et appropriées pour cerner l'information qui a probablement été obtenue à la suite de mauvais traitements.

Le niveau d'approbation requis pour échanger de l'information doit être proportionnel au risque de mauvais traitements. Plus le risque est grand, plus le niveau d'approbation est élevé.

Le SCRS est tenu d'informer de manière générale le ministre de la Sécurité publique de ses pratiques en matière d'échange d'information.

#### **4. Processus décisionnel lorsque l'échange d'information comporte un risque substantiel de mauvais traitements**

Sauf dans les cas où il existe un risque substantiel, le SCRS détermine les niveaux d'approbation requis en fonction des risques liés à l'échange de l'information avec des organismes étrangers. Le présent processus décisionnel s'applique uniquement lorsqu'il existe un risque substantiel que des mauvais traitements soient infligés à une personne.

Si le fait de communiquer de l'information à un organisme étranger ou d'obtenir de l'information de celui-ci soulève un risque substantiel que des mauvais traitements soient infligés et s'il n'est pas certain que le risque peut être atténué en utilisant des restrictions ou en obtenant des garanties, la décision d'échanger de l'information doit être rendue par le directeur.

Dans sa décision, le directeur tient normalement compte des renseignements ci-dessous, qui doivent tous être accompagnés d'une mention précisant leur exactitude et fiabilité :

- la menace pour la sécurité nationale et les intérêts canadiens, ainsi que la nature et le caractère imminent de cette menace;
- l'importance de l'échange de l'information en ce qui concerne la protection de la sécurité nationale ou d'autres intérêts canadiens;
- la relation entre le Canada et l'organisme étranger visé, et une évaluation du bilan en matière de respect des droits de la personne de cet organisme;
- les raisons de croire que l'échange de l'information pose un risque substantiel que des mauvais traitements soient infligés à une personne;
- les mesures proposées pour atténuer le risque et la probabilité que ces mesures soient efficaces (par exemple, le respect par le passé des garanties offertes par l'organisme étranger et la capacité des représentants du gouvernement de s'en acquitter);
- les vues du ministère des Affaires étrangères et du Commerce international;
- les vues d'autres ministères et organismes, au besoin, et tout autre fait pertinent dans les circonstances.

Le directeur peut demander au ministre de la Sécurité publique de décider s'il y a lieu d'échanger de l'information avec l'organisme étranger. Le cas échéant, les renseignements énumérés précédemment sont communiqués au ministre.

Le directeur ou encore le ministre de la Sécurité publique autorise l'échange de l'information avec l'organisme étranger seulement si cela ne contrevient pas à la présente instruction et aux obligations juridiques du Canada.

## **5. Utilisation de l'information ayant peut-être été obtenue à la suite de mauvais traitements infligés par des organismes étrangers**

Règle générale, il est interdit au SCRS d'utiliser sciemment de l'information obtenue à la suite de mauvais traitements infligés des organismes étrangers.

Dans des circonstances exceptionnelles, le SCRS peut être appelé à communiquer toute l'information en sa possession, y compris celle qui provient d'un organisme étranger et qui a été vraisemblablement obtenue à la suite de mauvais traitements, afin d'atténuer une menace sérieuse pouvant entraîner des pertes de vie, des blessures, des dommages graves ou la destruction de biens, et l'empêcher de se concrétiser. Dans de telles rares circonstances, le fait de ne pas tenir compte de cette information seulement en raison de la source constitue un risque inacceptable pour la sécurité publique.

En cas de menace sérieuse pouvant entraîner des pertes de vie, des blessures, des dommages graves ou la destruction de biens, le SCRS accordera la priorité à la protection de la vie et des biens. Dans le cas où le SCRS doit échanger de l'information vraisemblablement obtenue à la suite de mauvais traitements avec les responsables autorisées pour atténuer une menace sérieuse, il incombe au directeur de prendre une décision à cet égard. D'ailleurs, toutes les décisions doivent respecter la présente instruction et les obligations juridiques du Canada.

Le SCRS prend des mesures raisonnables pour atténuer le risque que les mesures qu'il mettra en place aient pour effet de préconiser ou d'autoriser les mauvais traitements. Il doit également prendre des mesures pour décrire avec exactitude les informations obtenues à la suite de mauvais traitements et pour en caractériser la fiabilité. Le SCRS impose l'utilisation des restrictions en ce qui concerne à l'échange d'information avec des organismes canadiens ou étrangers afin d'en limiter l'utilisation, selon le cas.

## **6. Soutien**

Pour assurer une compréhension uniforme des risques liés à l'échange d'information avec des organismes étrangers, le MAECI continuera de mettre à la disposition des organismes du renseignement et d'application de la loi ses rapports sur le respect des droits de la personne par les pays.

RECEIVED BY CSIS UNDER THE  
ACCESS TO THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REÇU PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION





Director - Directeur

AUG 30 2011

TS

**MEMORANDUM FOR THE MINISTER**

**RE: Intelligence Assessments**

For your information, I am attaching three Intelligence Assessments and one Threat Assessment.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
TRAVÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

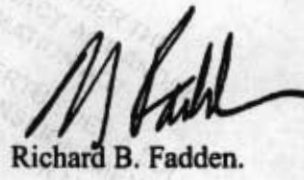
PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
TRAVÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

.../2

PROCESSED BY CRIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

We would be pleased to brief further on any of the above, should you have any questions.

PROCESSED BY CRIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.



Richard B. Fadden.

Encl.

PROCESSED BY CRIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

TRANSMITTAL SLIP / NOTE D'ENVOI

To / A <b>Director</b>	Classification <b>TOP SECRET</b>
From / De <b>ADP</b>	File / Dossier
Drafting officer / Rédacteur	Date <b>2012-01-24</b>

Subject / Sujet  
**CSIS Views on the Inspector General's 2010-11 Certificate**

Action / Donnez suite	Priority / Priorité	Deadline / Délai
<input checked="" type="checkbox"/> Signature	<input type="checkbox"/> Routine	<b>2012-01-26</b>
<input type="checkbox"/> Comments / Commentaires	<input type="checkbox"/> Urgent	
<input type="checkbox"/> Approval / Approbation	<input type="checkbox"/> Immediate / Immédiate	
<input type="checkbox"/> Information		

Record of Consultation Rapport de consultation	Concur D'accord	Comments / Commentaires
	Yes / Oui	
	No / Non	

	X	<p>The attached letter to the Minister of Public Safety provides context and clarification to issues raised in the Inspector General's 2010-11 Certificate.</p> <p style="text-align: center;"><b>CSIS / SCRS</b> FEB -1 2012 ✓</p> <p style="text-align: center;"><b>DIR</b></p> <p style="text-align: center;"><b>CSIS / SCRS</b> JAN 26 2012</p> <p style="text-align: center;"><b>ADP / DAP</b>      CSIS / SCRS JAN 26 2012</p> <p style="text-align: right;">STRATPOL</p>
--	---	---



Director - Directeur

CCM #10940  
TOP SECRET  
For Information

FEB 02 2012

**MEMORANDUM TO THE MINISTER**

**CSIS VIEWS ON THE INSPECTOR GENERAL'S 2010-11 CERTIFICATE**

**SUMMARY**

- In her 2010-11 Certificate, the IG notes that the Service has not acted beyond the framework of its statutory authority, contravened any Ministerial Directions, nor exercised its powers unreasonably or unnecessarily;
- The 2010-11 Certificate is similar to those of years past in that it fairly presents the IG's findings; with a few exceptions discussed in this note, the Service generally accepts as reasonable the recommendations proposed therein and has already implemented (or is currently in the process of implementing) them where appropriate;
- While the IG's review identified some instances of non-compliance and minor errors (which have since been corrected where possible and appropriate), these were mainly administrative in nature and not findings that the Service deliberately contravened any law, MD or policy or intended to mislead or conceal the Service's activities.

**BACKGROUND:**

This note provides context and Service comment on some of the Inspector General's (IG) findings and other issues noted in her 2010-11 Certificate, dated 30 November 2011 and delivered previously and under separate cover by the IG to your office.

The reviews conducted by IG staff covered material from 1 October 2009 to 30 September 2010 and focused on CSIS compliance with the *CSIS Act*, Ministerial Direction, operational policy, and on whether CSIS activities were reasonable and necessary. In addition to these reviews, the IG was also provided with my annual letter to you outlining CSIS' operational activities for the last fiscal reporting period (1 April 2010 to 31 March 2011), in accordance with Section 33(1) of the *CSIS Act*.

**DISCUSSION:**

Overall, the Service views the 2010-11 Certificate as similar to those of years past in that it fairly presents the IG's findings and the Service generally accepts as reasonable most of the recommendations proposed therein. It confirms that the Service has acted lawfully, reasonably, and within its statutory authority. Where concerns or errors are noted, there is no indication from the IG that she believes that the Service deliberately contravened any law, MD or policy or intended to mislead or conceal its activities.

The IG's Certificate identified some clerical/administrative errors, which have since been corrected where possible and appropriate. Where errors were found to have resulted from technical issues, or could be remedied by a technical fix, those measures have been undertaken.

The Service has corrected those errors and is creating an automated system that will prevent them from re-occurring in the future.

As in previous years' certificates, the 2010-11 Certificate does not include important contextual information around errors or incidents of non-compliance,

nor does it differentiate between serious and more administrative issues. The Service believes a distinction can and should be drawn between the two. The IG is of the opinion, however, that since the Service does not rank-order its policies (e.g. standard administrative policies vs. operations policies guiding high-risk activities), nor should she rank-order what she sees as instances of non-compliance with them. This difference in views has been a matter of long-standing disagreement between the Service and the IG.

There are other specific issues contained in the Certificate that merit clarification or explanation:

2) **Policy on operational reporting:** In last year's assessment, the IG noted that CSIS' policy framework for approval of operational reports lacked clarity and implied that another level of review would be beneficial. The Service confirmed that the policy would be modified to bring clarity to the approval process. Currently under review, the policy will allow greater flexibility to intelligence officers in filing their messages without approval, when operationally necessary, to avoid delays in uploading critical or time sensitive information. The new policy will not entail less supervision, but flexibility such that, for example, acting supervisors can approve their own messages without violating policy. There will continue to be the requirements of attention to detail and seeking approvals when possible and appropriate.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

With the exception of the issues raised above, the Service largely agrees with the IG's recommendations and has already implemented (or is currently in the process of implementing) them, and undertaking measures that will fill the gaps identified.

I am available to further discuss the Service's response should you wish.



Richard B. Fadden

c.c. Deputy Minister, Public Safety

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be projected by the provisions of section 37(1) and 38(1) of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with CSIS.

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

JAN 18 2011

SECRET

Dear Director Fadden, Commissioner Elliott and President Portelance:

I am writing to you today to ensure that you are aware of the high priority the Government accords to issues regarding marine mass arrivals and human smuggling.

In response to the challenges which mass arrivals and human smuggling continue to pose to Canada's national security, the Government has taken decisive steps, that include the tabling of legislation in Parliament (Bill C-49), appointing a Special Advisor on Human Smuggling and Illegal Migration,

As you well know, the challenge of human smuggling is complex and requires a whole of government response. In this regard, it is my responsibility under section 5 of the *Department of Public Safety and Emergency Preparedness Act* to coordinate the activities of, and establish strategic priorities for, agencies within the Public Safety portfolio, including the Royal Canadian Mounted Police, Canadian Security Intelligence Service and the Canada Border Services Agency. Effective coordination between government agencies and departments, taking into account each other's respective interests and mandates, is absolutely essential if we are to successfully prevent and deter future human smuggling ventures destined for Canada, as well as to investigate and prosecute those who profit from these crimes.

As the Minister responsible for public safety and accountable to Parliament, I expect that you will work collaboratively in countering mass arrivals and human smuggling. Your combined efforts thus far have been highly commendable, and I trust that the Government can continue to have your fullest support and attention on this important issue.

Sincerely,

Vic Toews, P.C., Q.C., M.P.

CSIS / SCRS

99

JAN 24 2011

DIR

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

APR 21 2011

**BY HAND**

**SECRET**

Mr. Richard Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Gloucester, Ontario K1J 1B7

**CSIS / SCRS**

28

**DR**

Dear Mr. Fadden:

I am writing in response to your correspondence dated November 29, 2010, requesting the authority to re-activate a foreign liaison arrangement between the Canadian Security Intelligence Service (CSIS) and

I have consulted my colleague, the Honourable Lawrence Cannon, Minister of Foreign Affairs. In a letter dated April 7, 2011, Mr. Cannon indicated to me that he concurs with the re-activation of a liaison arrangement between CSIS and and has requested that his officials be briefed on the progress and usefulness of the arrangement.

In this regard, pursuant to paragraph 17(1)(b) of the *CSIS Act* and as required by Ministerial Direction on foreign liaison, I authorize CSIS to re-activate an arrangement with

A copy of this letter is being provided to the Chair of the Security Intelligence Review Committee.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

c.c.: Dr. Arthur T. Porter, P.C., M.D.

**Canada**



Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

SEP 09 2011

**SECRET**

**BY HAND**

Mr. Richard Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Gloucester, Ontario K1J 1B7

Dear Mr. Fadden:

I am writing in response to your correspondence dated August 3, 2011, seeking approval for the Canadian Security Intelligence Service (CSIS) to enter into a domestic arrangement on cooperation with

This arrangement will allow CSIS to

In this regard, pursuant to paragraph 17(1)(a) of the *CSIS Act* and as required by Ministerial Direction on domestic liaison, I authorize CSIS to enter into a domestic arrangement with

I would like to receive a copy of the signed Memorandum of Understanding between CSIS and

A copy of this letter is being provided to the Chair of the Security Intelligence Review Committee.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

SEP 09 2011

**SECRET**

**BY HAND**

Mr. Richard Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Gloucester, Ontario K1J 1B7

Dear Mr. Fadden:

I am writing in response to your correspondence dated August 11, 2011, seeking approval for the Canadian Security Intelligence Service (CSIS) to enter into a domestic arrangement on cooperation with Public Works and Government Services Canada (PWGSC) regarding the International Traffic in Arms Regulations (ITAR).

In this regard, pursuant to paragraph 17(1)(a) of the *CSIS Act* and as required by Ministerial Direction on domestic liaison, I authorize CSIS to enter into a domestic arrangement with PWGSC.

I would like to receive a copy of the signed Memorandum of Understanding between CSIS and PWGSC.

In accordance with sub-section 17(2) of the *CSIS Act*, a copy of this letter is being provided to the Chair of the Security Intelligence Review Committee.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

Mr. Richard B. Fadden  
Director, CSIS  
P.O. Box 9732  
Ottawa, Ontario.  
K1G 4G4

CSIS / SCRS

JUN 21 2011

DIR

Dear Mr. Fadden,

I was pleased to have the opportunity to meet with you during our bilateral discussion last week. I believe there is great value in such face-to-face discussions and I look forward to ongoing collaboration as we work to keep Canadians safe.

Further to our meeting, I am writing to ask that you provide the name of an individual with whom my office can liaise on an on-call basis starting immediately. Specifically, I am asking that the contact be available to my Issues Manager and primarily between the hours of 5:00 am and 3:00 pm, although there is potential for contact beyond those times.

I ask that you forward the contact details of this individual to my Chief of Staff, Andrew House, by Wednesday, June 22<sup>nd</sup>. If you have already done so, thank you for your co-operation.

Yours sincerely,

Hon. Vic Toews, P.C., Q.C., M.P.

Canada

DDA

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

CSIS / SCRS

FEB 01 2012

FEB -6 2012

DIR

*OK  
Mont OPA*

Richard Fadden  
Director  
Canadian Security Intelligence Service  
Station T, PO Box 9732  
Ottawa, ON  
K1G 4G4

Dear Director:

As you are aware, our Government is working to reduce wasteful spending with a view to returning to balanced budgets as soon as possible. We have taken strong action in this area, notably with the Strategic Review and currently with the Deficit Reduction Action Plan.

Leadership must start at the top on this matter, as eliminating wasteful spending is one of this Government's key priorities. As a result, the salaries and office budgets of all Ministers and members of Parliament have been frozen.

I expect the same type of leadership from senior public servants in the Public Safety portfolio. Recently, it came to my attention that agencies had engaged in what I would refer to as inappropriate spending in order to rent space for executive conferences and retreats. Therefore, I would ask that you take two specific actions. Firstly, I would ask that, in general, you seek to limit the discretionary travel budget of your agency. We must work together to ensure that in all cases taxpayer dollars are spent in the most efficient and effective way possible. Secondly, going forward please seek approval from my office for proposed expenditures in excess of \$5,000 that could be classified as being related to executive retreats, conferences or meetings. This includes, but is not limited to:

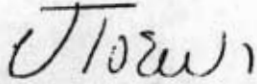
- renting space for retreats or conferences;
- accommodation for executive retreats or conferences;
- catering for executive retreats or conferences; or
- travel associated with executive retreats or conferences.

I will ask my officials to update the relevant delegations of financial authority to reflect this direction. I trust that compliance with this important initiative to safeguard taxpayer dollars will begin immediately.

Canada

Please advise me as to any concerns you may have with regard to implementation.

Sincerely,



Vic Toews, P.C., Q.C., M.P.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

ADP.

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

NOV 03 2011

**BY HAND**

**SECRET//CEO**

Mr. Richard Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Gloucester, Ontario K1J 1B7

Dear Mr. Fadden:

I am writing in response to your correspondence dated August 3, 2011, requesting the authority to establish a foreign liaison arrangement between the Canadian Security Intelligence Service (CSIS) and

I have consulted with my colleague, the Honourable John Baird, Minister of Foreign Affairs, who by letter dated October 20, 2011, concurs with the establishment of a foreign liaison arrangement between CSIS and He has requested that his officials be briefed on the progress and usefulness of the arrangement.

In this regard, pursuant to paragraph 17(1)(b) of the *CSIS Act* and as required by Ministerial Direction on foreign liaison, I authorize CSIS to establish an agreement with

A copy of this letter is being provided to the Chair of the Security Intelligence Review Committee.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

C.c.: The Honourable Arthur T. Porter, P.C., M.D.  
Chair, Security Intelligence Review Committee

**CSIS / SCRS**

NOV 04 2011

**DIR**

**Canada**



**CSIS / SCRS**

Minister of Public Safety

Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

**DIR**

SECRET

AVG 16 2011

Mr. Richard Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Gloucester, Ontario K1J 1B7

① CC  
ADP  
DOP  
DPA  
ADK  
MM

Dear Mr. Fadden,

Thank you for your letter, outline the Canadian Security Intelligence Service's (CSIS) key policy priorities, and providing an update of the current threat environment.

Yours sincerely,

*V Toews*

Vic Toews, P.C., Q.C., M.P.

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

**CSIS / SCRS**

Mar 31 2011

**DIR**

MAR 24 2011

CC ADP  
DPA

Mr. Richard B. Fadden  
President  
Canadian Security Intelligence Service  
PO Box 9732  
Station T  
Ottawa, ON K1G 4G4

Dear Mr. Fadden:

On behalf of my staff and the government as a whole, I would like to take a moment to express my sincere appreciation to you and your staff for the truly admirable effort that went into the preparation of what was, in my estimation, a very fulsome response to the

Having reviewed the information in its entirety, I note the care and dedication that went into this exercise.

The Service should be proud of the high quality work that was produced under difficult circumstances, as well as the professionalism with which it was carried out. I know this task was both onerous and daunting, and I am truly grateful for the many hours of work that went into it. I would ask that you forward this to the appropriate people in your organization, with my sincere thanks.

Yours truly,

Vic Toews  
P.C., Q.C., M.P.

**Canada**



Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

JUL 28 2011

**BY HAND**

Mr. Richard Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Gloucester, Ontario K1J 1B7

**CSIS / SCRS**

**DIR**

Dear Mr. Fadden:

I am writing in response to your correspondence dated July 6, 2011, seeking approval for the Canadian Security Intelligence Service (CSIS) to enter into a domestic framework arrangement on cooperation with

In this regard, pursuant to paragraph 17(1)(a) of the *CSIS Act* and as required by Ministerial Direction on domestic liaison, I authorize CSIS to enter into a framework arrangement with

I would like to receive a copy of the signed Memorandum of Understanding between CSIS and any subsequent working agreements that may arise out of the proposed framework arrangement with

A copy of this letter is being provided to the Chair of the Security Intelligence Review Committee.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

A  
CC { AOP  
AOL  
DPO  
SECRET

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

FEB 15 2011

**BY HAND**

**SECRET**

Mr. Richard Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Gloucester, Ontario K1J 1B7

Dear Mr. Fadden:

I am writing in response to your correspondence dated November 29, 2010 requesting the authority to establish a liaison arrangement between the Canadian Security Intelligence Service (CSIS) and

I have consulted with my colleague, the Honourable Lawrence Cannon, Minister of Foreign Affairs. In a letter dated January 26, 2011, Mr. Cannon indicated to me that he concurs with the establishment of a liaison arrangement between CSIS and

In this regard, pursuant to paragraph 17(1)(b) of the *CSIS Act* and as required by Ministerial Direction on foreign liaison, I authorize the Service to establish an agreement with

A copy of this letter is being provided to the Chair of the Security Intelligence Review Committee.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

c.c.: Dr. Arthur T. Porter, P.C., M.D.

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

AOP  
DDJ  
AOC

FEB 15 2011

**BY HAND**

**SECRET**

Mr. Richard Fadden  
Director  
Canadian Security Intelligence Service  
1941 Ogilvie Road  
Gloucester, Ontario K1J 1B7

Dear Mr. Fadden:

I am writing in response to your correspondence dated November 25, 2010 requesting the authority to establish a liaison arrangement between the Canadian Security Intelligence Service (CSIS) and

I have consulted with my colleague, the Honourable Lawrence Cannon, Minister of Foreign Affairs. In a letter dated January 26, 2011, Mr. Cannon indicated to me that he concurs with the establishment of a liaison arrangement between CSIS and

In this regard, pursuant to paragraph 17(1)(b) of the *CSIS Act* and as required by Ministerial Direction on foreign liaison, I authorize the Service to establish an agreement with

A copy of this letter is being provided to the Chair of the Security Intelligence Review Committee.

Yours sincerely,

Vic Toews, P.C., Q.C., M.P.

c.c.: Dr. Arthur T. Porter, P.C., M.D.

Canada

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

PROCESSED BY /  
TRAITE PAR LE SERVICE  
DES RENSEIGNEMENTS DE LA LOI SUR  
L'ACCÈS À L'INFORMATION

**SECRET**  
**CCM # 8421**  
**For Information**

FEB 15 2011

**MEMORANDUM TO THE MINISTER**

**SERVICE EFFORTS AND ACHIEVEMENTS IN THE  
MITIGATION OF ILLEGAL MIGRATION BY SEA**

**SUMMARY**

**BACKGROUND:**

The arrival of two human smuggling vessels from Southeast Asia, the *OceanLady* in October 2009, followed by the *SunSea* in August 2010, has posed potential national security and terrorism-related threats to Canada.

In response to your letter of January 18, 2011, I can assure you that the Service continues to work both at home and abroad to support the whole-of-government strategy to deter and prevent international human smuggling ventures to Canada. We are committed to providing the

government with information and advice to assist in preventing future illegal vessels from arriving at our shores. This is being achieved through continued close collaboration and liaison with the RCMP and the Canada Border Services Agency (CBSA), as well as other government departments and our international partners as outlined below.

**DISCUSSION:**

CSIS is continuing to support the whole-of-government strategy to deter and prevent human smuggling ventures overseas

The Service also continues to investigate links to human smuggling within Canada, and to work closely with government partners

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

In addition to this close collaboration with CBSA, the Service is also continuing to work closely with the Royal Canadian Mounted Police (RCMP).

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

Consistent with your written direction dated January 18, 2011, the Service will continue to play a key and collaborative role with the whole-of-government efforts to prevent illegal migration and human smuggling.



Richard B. Fadden

Enclosures: 2

- c.c.: Deputy Minister of Public Safety
- c.c.: National Security Advisor to the Prime Minister

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

**SECRET**  
**CCM# 8479**  
**For Information**

**FEB 21 2011**

**MEMORANDUM TO THE MINISTER**

**2011 CRICKET WORLD CUP**

**BACKGROUND:**

The 10<sup>th</sup> Cricket World Cup (CWC) tournament will take place from February 19<sup>th</sup> to April 2<sup>nd</sup>, 2011 at venues across India, Sri Lanka and Bangladesh. Canada will be participating with a team of 15 players and approximately eight support staff, who will be required to travel between the three countries for training and participation in various matches. While the sport is popular among Canada's South Asian expatriate community, the number of Canadian spectators who will travel to the region for the event is not known.

**DISCUSSION:**

The Integrated Threat Assessment Centre (ITAC), which is responsible for assessing the terrorist threat to Canadian interest at home and abroad,



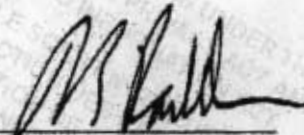
The threat environment in South Asia is complex and consists of several religious and political extremist organizations. In recent years, there have been many notable attacks and threats against sporting targets in South Asia:

- In March 2009, an attack on buses carrying members of the Sri Lankan Cricket team killed seven people while on route to a match in Lahore, Pakistan;
- On 17 February 2010, prominent Islamist extremist and Al Qaeda associate Ilyas Kashmiri issued a threat against sporting events in India.
- In March 2010, two bombs exploded at an Indian Premier League cricket match in Bangalore in the southern Indian state of Karnataka; and,

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCES  
A L'INFORMATION.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCES  
A L'INFORMATION.

I promise to keep you informed of any threat-related developments.



Richard B. Fadden

Enclosures: 2

- c.c.: National Security Advisor to the Prime Minister
- c.c.: Deputy Minister of Public Safety
- c.c.: Deputy Minister of Foreign Affairs

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION.

THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO MANDATORY EXEMPTION UNDER THE ACCESS TO INFORMATION ACT OR THE PRIVACY ACT. THE INFORMATION OR INTELLIGENCE MAY ALSO BE PROTECTED BY THE PROVISIONS OF SECTION 37(1) and 38(1) OF THE CANADA EVIDENCE ACT. THE INFORMATION OR INTELLIGENCE MUST NOT BE DISCLOSED OR USED AS EVIDENCE WITHOUT PRIOR CONSULTATION WITH THE CANADIAN SECURITY INTELLIGENCE SERVICE.



Integrated Threat Assessment Centre

Centre intégré d'évaluation des menaces

THREAT

L A S E R

ALERT

11 / 20-E  
2011 01 21

UNCLASSIFIED - For Official Use Only

### The 2011 Cricket World Cup in South Asia

#### KEY POINTS

- The 10<sup>th</sup> Cricket World Cup (CWC) tournament will be held in various venues across India, Sri Lanka and Bangladesh from 2011 02 19 to 2011 04 02. Canada is participating, with a team comprised of 15 players and approximately 8 support staff. The number of Canadian spectators who will travel to South Asia is not known. However, cricket is a popular sport among Canada's South Asian expatriate communities.

## ANALYSIS

1) The 10<sup>th</sup> Cricket World Cup (CWC) tournament will be held in various venues across India, Sri Lanka and Bangladesh from 2011 02 19 to 2011 04 02. Canada is participating, with a team comprised of 15 players and approximately 8 support staff. The number of Canadian spectators who will travel to South Asia is not known. However, cricket is a popular sport among Canada's South Asian expatriate communities.

2) Canada is scheduled to play matches in the following locations, on the following dates:

Date	Teams	Venue
2011 02 20	Canada vs. Sri Lanka	Hambantota, Sri Lanka
2011 02 28	Canada vs. Zimbabwe	Nagpur, India
2011 03 03	Canada vs. Pakistan	Colombo, Sri Lanka
2011 03 07	Canada vs. Kenya	New Delhi, India
2011 03 13	Canada vs. New Zealand	Mumbai, India
2011 03 16	Canada vs. Australia	Bangalore, India

### India

3)

According to open source reporting, there were approximately 1866 casualties of terrorist or insurgent violence in India in the year 2010, out of which 746 were civilians, 360 security personnel and 760 militants. The majority of these casualties were a result of domestic insurgency.

4)

The LeT has been responsible for numerous attacks against the Indian government, security forces and civilians in Kashmir. The LeT has been accused also by the Indian government of involvement in a number of recent attacks in the rest of India, such as the Mumbai commuter train bombings in July 2006 that killed 200 people and injured more than 600, and the November 2008 ten-man suicide attack in Mumbai, using mainly small arms, which, according to Indian officials, killed 172 people, including two Canadians and 16 other foreigners, and wounded at least 300 others. For the past two years, India has been on

alert for follow-on attacks expected to incorporate the same commando-style tactics.

5) The Indian Mujahideen (IM), another terror group that operates in India, has claimed responsibility for several attacks in recent years, including a shooting attack in New Delhi on 2010 09 19 that injured two Taiwanese tourists. The group claimed that further attacks were planned to occur during the 2010 Commonwealth Games, which were to start in New Delhi several weeks later.

6) During the 2010 Commonwealth Games, there were no reported terrorist incidents. However, the success of that event was underpinned by complex security preparations and mass mobilization of security personnel.

#### *Recent Extremist Attacks Targeting Cricket Matches*

9) On 2009 03 03, the Sri Lankan cricket team, along with their police escorts, were attacked as they transited through Lahore, Pakistan. The attack involved elements of several different regional terrorist groups, including Lashkar-e-Jhangvi (LeJ) and Tehrik-e-Taliban (TTP). The attackers were armed with assault rifles, hand grenades and several rocket-propelled grenade launchers. 7 Pakistani police officers were killed in the attack, and 8 players or officials were wounded.

10) More recently, on 2010 04 17, two crudely constructed bombs were detonated outside the Chinnaswamy Stadium in Bangalore, India, injuring 14 people. The incident occurred shortly before an Indian Premier League cricket match which included Australian players. Police were

later able to find three more devices in the area surrounding the stadium.

13) ITAC continues to monitor all sources of information and will provide updates as necessary.

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

This document is the property of the Integrated Threat Assessment Centre (ITAC). Prepared by ITAC, it is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to those with appropriate security clearances and appropriate security systems to retain the information. It must not be reclassified or reused, in any way, in whole or in part, without the consent of the originator. Any feedback should be directed via email to CSIS-ITAC

Contact: ITAC through CGOC / Threat Triage Centre

at



INTEGRATED THREAT ASSESSMENT CENTRE

CENTRE INTEGRÉ D'ÉVALUATION DES MENACES

THREAT ASSESSMENT

11 / 05 - E

2011 01 28

This document is classified SECRET and is the property of the Integrated Threat Assessment Centre (ITAC). Prepared by ITAC, it is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to those with appropriate security clearances and appropriate security systems to retain the information. It must not be reclassified or reused, in any way, in whole or in part, without the consent of the originator. Any feedback should be directed via email to CSIS-ITAC Triage Centre at Contact: ITAC through CGOC / Threat

2011 CRICKET WORLD CUP - INDIA, BANGLADESH & SRI LANKA

Key Points

- The 2011 Cricket World Cup is scheduled to take place from 2011 02 19 to 2011 04 02 in India, Bangladesh, and Sri Lanka. The Canadian cricket team is scheduled to compete in two training matches in Bangladesh, four official matches in India, and two official matches in Sri Lanka.
- The threat environment in South Asia is complex and consists of several religious and political extremist organizations.



### **Introduction**

1. The 2011 Cricket World Cup (CWC) is scheduled to take place from 2011 02 19 to 2011 04 02 with matches taking place in India, Bangladesh, and Sri Lanka. The Canadian cricket team is scheduled to play four matches in India and two in Sri Lanka, with the possibility of further matches should the team progress beyond the initial round.

### **Sporting Events and Soft Targets**

3. In recent years, there have been many notable attacks against sporting targets in South Asia. In March 2009, an attack on buses carrying members of the Sri Lankan Cricket team killed seven people while on route to a match in Lahore, Pakistan.

4. In March 2010, two bombs exploded at an Indian Premier League (IPL) cricket match in Bangalore in the southern Indian state of Karnataka. Police later discovered three more unexploded devices in the area around the stadium. While there were no fatalities, at least 14 people were injured.

5. On 2010 02 17, prominent Islamist extremist and Al Qaeda (AQ) associate Ilyas Kashmiri issued a threat against sporting events in India. Specifically, Kashmiri warned foreigners against travelling to India to take part in the 2010 Field Hockey World Cup, IPL cricket matches, and the 2010 Commonwealth Games.

6. Soft targets refer to areas and facilities that lack strong security protection such as hotels, restaurants, and public spaces. Two prominent examples of attacks against soft targets include the storming attacks in Mumbai in November 2008 and the February 2010 bombing of the German Bakery in Pune. The Mumbai attacks resulted in the deaths of over 160 people, including 2 Canadians, while the Pune bombing led to 17 deaths, including 5 foreigners.

**India**

*Domestic Indian Islamists*

9. In 2010, there were a number of attacks within India which were likely carried out by domestic Islamist extremists. In addition to the bombing of the German Bakery in Pune, there was also a shooting of two Taiwanese tourists in New Delhi in September and a bombing at a religious site in Varanasi in December which killed one person.

10. Following the New Delhi and Varanasi incidents, the Indian Mujahideen (IM), the most prominent domestic Indian Islamist extremist organization, issued statements claiming responsibility. Moreover, the Indian police have identified two members of the group as key suspects in The German Bakery bombing. According to open media reporting, Indian authorities believe that the IM may have been planning an attack against the CWC as well.

*Lashkar-e-Tayyiba*

11.

The LeT has been responsible for numerous attacks against the Indian government, security forces, and civilians in the state of Jammu and Kashmir. The LeT has also been accused of perpetrating the November 2008 attacks in Mumbai.

*Al Qaeda*

12. In addition to the public threat issued by Ilyas Kashmiri in February 2010, a statement made by the late Sheik Sa'id al-Misri, a high ranking member of AQ, was posthumously released in June, in which al-Misri praises the actions of "one heroic soldier" who carried out the attack against the German Bakery. Al-Misri's statement claimed that the attack was undertaken by a group under the banner of the previously unknown *Qaedat al-Jihad Kashmir* (AQ in Kashmir), a group led by Ilyas Kashmiri.

*Naxalites/Communist Party of India -Maoist*

13. Naxalites are Maoist insurgents active throughout much of eastern India. The most prominent organization within the Naxalite movement is the Communist Party of India-Maoist (CPI-M).

The CPI-M operates primarily in the eastern states of Andhra Pradesh, Chhattisgarh, Jharkhand, Orissa, Madhya Pradesh, Bihar and West Bengal. While only one of the CWC host cities, Kolkata, lies within one of these states, many others such as Nagpur, Maharashtra and Chennai, Tamil Nadu are located relatively near to areas of Naxalite influence. On 2011 02 28, the Canadian team is scheduled to play Zimbabwe in Nagpur.

14. In 2010, there were a number of high profile Naxalite attacks. These attacks are notable in their scale of lethality, exemplified by an attack reported in open media on 2010 04 06 on a camp in the state of Chhattisgarh. The attack killed over 70 security service personnel. On 2010 05 17, a bomb attack against a bus carrying a number of police and civilians resulted in over 30 deaths, and a Naxalite associated group is suspected of being responsible for sabotaging a section of railway in the state of West Bengal that resulted in over 140 deaths on 2010 05 28.

#### *Tamil Nationalists*

17. According to open sources, a section of railway in Tamil Nadu was sabotaged in June 2010, causing physical damage but no casualties. Although LTTE related literature was found at the site, the motives and identities of the perpetrators remain unknown.

#### **Bangladesh**

*Jamaat ul Mujahideen Bangladesh*

19. Like HuJI-B, JMB has not carried out any successful attacks in recent years. However, in August 2005, the organization successfully conducted a massive coordinated bombing involving 459 explosive devices being detonated across Bangladesh, resulting in numerous injuries and 2 fatalities. While the event highlighted a significant organizational capability, it also sparked a government crackdown resulting in the arrest and execution of the JMB leadership in 2007.

*Harakat ul Jihad i Islami Bangladesh*

20. Although it is believed to have historic ties to a number of Islamist extremist organizations in South Asia, including AQ, HuJI-B has not carried out any large scale attacks in Bangladesh in recent years. According to open sources, the organization has been damaged by Bangladeshi counter-terrorism operations, but is still believed to have thousands of members in the country, and strong ties to the Chittagong area.

*Lashkar-e-Tayyiba*

22. According to open media reporting on 2010 10 05, Bangladeshi police arrested 3 alleged LeT members in Dhaka. Two of the individuals were Pakistani, while the third, a Bangladeshi, also had links to HuJI-B and JMB, according to a police spokesman.

**Canadian Interests**

26. The Canadian cricket team is scheduled to play two matches in Bangladesh, four in India and two in Sri Lanka.

and B for more information on the CWC schedule).

(Refer to Appendices A

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
TRAITE PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

Appendix A

<b>Scheduled Canadian Matches</b>		
<b>Opponent</b>	<b>Location</b>	<b>Date</b>
Bangladesh (Practice Match)	Zahur Ahmed Chowdhury Stadium - Chittagong, Bangladesh	2011 02 12
England (Practice Match)	Narayngonj - Khan Saheb Stadium - Narayangani, Bangladesh	2011 02 16
Sri Lanka	Mahinda Rajapaksa International Cricket Stadium - Hambantota, Sri Lanka	2011 02 20
Zimbabwe	Vidarbha Cricket Association Ground - Nagpur, India	2011 02 28
Pakistan	R. Premadasa International Cricket Stadium - Columbo, Sri Lanka	2011 03 03
Kenya	Feroz Shah Kolta Stadium - New Delhi, India	2011 03 07
New Zealand	Wankhede Stadium - Mumbai, India	2011 03 13
Australia	M. Chinnaswamy Stadium - Bangalore, India	2011 03 16

Appendix B

<b>Finals</b>		
<b>Game</b>	<b>Location</b>	<b>Date</b>
1 <sup>st</sup> Quarter Final	Shere Bangla National Stadium - Dhaka, Bangladesh	2011 03 23
2 <sup>nd</sup> Quarter Final	Sardar Patel Gujarat Stadium - Ahmedabad, India	2011 03 24
3 <sup>rd</sup> Quarter Final	Shere Bangla National Stadium - Dhaka, Bangladesh	2011 03 25
4 <sup>th</sup> Quarter Final	R. Premadasa Stadium - Colombo, Sri Lanka	2011 03 26
1 <sup>st</sup> Semi Final	R. Premadasa Stadium - Colombo, Sri Lanka	2011 03 29
2 <sup>nd</sup> Semi Final	Punjab Cricket Association Stadium - Mohali, India	2011 03 30
Championship	Wankhede Stadium - Mumbai, India	2011 04 02

PROCESSED BY DAIS UNIVER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTUE DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service. Because disclosure of this document might be injurious to national security, the Canadian Security Intelligence Service objects to its disclosure before a court, person or anybody with jurisdiction to compel its production or disclosure. The Canadian Security Intelligence Service may take all the steps pursuant to the *Canada Evidence Act* or any other legislation to protect this information or intelligence from production or disclosure, including the filing of any necessary notices with the Attorney General of Canada.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION



Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM # 10441  
Unclassified  
For Information

NOV 21 2011

**MEMORANDUM TO THE MINISTER**

**UNITED KINGDOM JUSTICE AND SECURITY GREEN PAPER:  
SUMMARY AND ASSESSMENT**

**ISSUE:**

The Canadian Security Intelligence Service has prepared a summary and assessment of the United Kingdom's *Justice and Security Green Paper*, which examines challenges associated with national security-related civil proceedings.

**DISCUSSION:**

On 19 October 2011, the UK Secretary of State for Justice tabled in Parliament the *Justice and Security Green Paper*, which proposes a number of options to enhance procedural fairness, safeguard sensitive material and reform intelligence oversight in the context of civil proceedings that rely on national security information.

The enclosed summary and report are intended to contribute to ongoing discussions in the Canadian context, given that the community is grappling with similar challenges.

A handwritten signature in black ink, appearing to read 'R. Fadden', is written over a horizontal line.

Richard B. Fadden

Enclosures: 2

c.c.: Stephen Rigby, National Security Advisor  
William Baker, Deputy Minister, Public Safety Canada  
Neil Yeates, Deputy Minister, Citizenship and Immigration Canada  
Luc Portelance, President, Canada Border Services Agency  
Myles J. Kirvan, Deputy Minister, Justice Canada  
Morris Rosenberg, Deputy Minister of Foreign Affairs

## UK Justice and Security Green Paper – Strategic Policy Summary and Assessment

On 19 October, the United Kingdom's Secretary of State for Justice presented to Parliament a *Justice and Security Green Paper* on issues related to the treatment of sensitive, national security information in civil proceedings. Below is a summary of recommendations and points of interest to the Service, as well as an assessment of the paper, prepared by Strategic Policy.

### United Kingdom Justice and Security Green Paper

#### Summary

The *Justice and Security Green Paper* focusses on proposals to reconcile the need to protect sensitive national security information during civil proceedings with the claimant's right to procedural fairness. The paper follows a UK court ruling on similar issues, and Prime Minister Cameron's November 2010 announcement of measures to address outstanding issues and controversies related to terrorism investigations, including: a Government inquiry into alleged UK involvement in the abuse of detainees abroad; guidance to security and intelligence agencies on engagement with detainees held by third parties abroad; and, the Government's intent to settle the civil claims of former UK detainees of Guantanamo Bay.

The *Green Paper* examines and reports on multiple options for reform and is structured in three primary sections: enhancing procedural fairness, safeguarding material, and reform of intelligence oversight. Of these options, five are endorsed: the use of Closed Material Procedures in civil proceedings; increased training for Special Advocates; establishing the Intelligence and Security Committee as a statutory committee, and; expanding the remit of the Intelligence Services Commissioner to include a general responsibility for overseeing the effectiveness of operational policies.

The Service is not mentioned in the paper, but there are references in the appendices to Canada concerning "closed material proceedings" (page 53); the protection of sensitive information (page 61); and executive veto on the disclosure of sensitive information (page 63). Issues of disclosure related to criminal proceedings are not examined in this paper (see page 7) and intercept as evidence will be the subject of another government review (see page 11).

#### 1. Enhancing Procedural Fairness

The Government proposes the following in order to maximize the amount of relevant information presented in civil proceedings, enhance procedural fairness, and ensure the protection of sensitive material.

##### i) Expand Closed Material Procedures (pages 21-25)

Introduced in the UK in 1997 with respect to immigration deportation decisions, Closed Material Procedures (CMP) allow for the consideration of relevant "closed" material, the release of which would damage the public interest. Established following a European Court of Human Rights ruling that cited with approval the Canadian approach, CMPs involve Special Advocates and

provide an alternative to excluding sensitive information under the common law principle of Public Interest Immunity (PII) (i.e. evidence may be excluded if the public interest in withholding it outweighs the public interest in disclosing it). CMPs are used in immigration appeals, the Proscribed Organizations Appeal Commission, employment tribunal proceedings concerning national security, control order cases, counter-terrorism financial restriction proceedings, and sentence and parole review for Northern Ireland. (pages 52-53)

The Government proposes to introduce legislation to make CMPs available in civil cases when required. It also acknowledges that CMPs are rarely required in civil cases and does not rule out exclusion of sensitive information based on PII. Nevertheless, it lauds the procedure for "delivering procedural fairness" and reducing the "risk of damaging disclosure." (page 21) The paper identifies additional problems for potentially extending CMP to public inquests and inquiries, and the Government has requested public comment on these challenges. (pages 22-24)

#### ii) Improvements to the Special Advocate System (pages 25-27)

The Government proposes to increase training for Special Advocates where required. Current training provided by the Security Service explains intelligence processes, the assessment of intelligence, and the prioritisation of investigations. While Special Advocates have expressed satisfaction with available training, the Government seeks to add refresher courses for experienced Special Advocates, along with training on specific issues arising in CMPs. (page 25) In anticipation of an increase in CMPs, the Government will also provide Special Advocates with more independent junior legal support. (page 25) The Government continues to study potential options for addressing the concerns of Special Advocates regarding their restricted ability to communicate with their clients. (pages 25-27)

#### iii) Clarifying Disclosure Requirements (pages 27-29)

The paper also is reviewing the benefits of introducing legislation that would clarify when it is necessary to provide an individual with information, however sensitive, to enable them to give instructions to their Special Advocate. The paper does not, however, state if the Government will introduce such legislation.

The Government also reviewed and rejected the following proposals: more active case management for judges (pages 28, 29); specialist court structures (pages 29, 30); and changes to the remit of the Investigatory Powers Tribunal. (pages 30-32)

## 2. Safeguarding Material

#### i) Legislating Public Interest Immunity (pages 33, 34)

In considering whether to introduce legislation to enshrine the PII principle, the Government assessed that related statutory presumptions would privilege the protection of certain types of material and diminish the protection afforded to other types. Further, it was assessed that PII legislation would not represent an improvement over the existing convention of judicial deference to executive advice on national security. (page 34). The preference, therefore, is for

the Government to continue to rely on the convention of PII when warranted, while noting that the wider use of CMPs will likely reduce the number of these cases.

ii) Court-ordered Disclosure into Foreign Proceedings (pages 35-37)

This section addresses a special category of civil claims, *Norwich Pharmacal* applications, that enables claimants to obtain the disclosure of information from defendants who are involved, innocently or not, in the arguable wrongdoing of a third party. (See page 15) *Norwich Pharmacal* applications have been used in attempts to obtain sensitive information from domestic UK agencies for use in foreign proceedings involving national security partners, the release of which would be damaging to national security and could undermine security cooperation. (page 35) With respect to this issue, the Government seeks public views on two proposals: an exemption for material that could damage the public interest, including material held or originating from UK agencies (page 36); and, legislation to clarify the requirements claimants must satisfy to bring forth the application. (pages 35, 36)

### 3. Reform of Intelligence Oversight

i) Parliament: The Intelligence and Security Committee (pages 40-44)

The Intelligence and Security Committee (ISC) of Parliament has been criticized for its lack knowledge of agency operational work; the insufficient transparency of its appointment, operations, and reporting practices, and; its lack of independence (the ISC reports to the Prime Minister). The Green Paper seeks to answer these criticisms.

The Government proposes that the ISC be made a statutory committee of Parliament, reporting formally to Parliament, while also maintaining current reporting practices to the PM and existing measures to protect sensitive material. (page 41,42) The Government is carefully considering the ISC's proposal to extend its remit to cover operational activities, and proposes that the ISC adopt a wider role to oversee the work of bodies operating under the Ministry of Defence, the Cabinet Office and the Home Office related directly to intelligence materials. (page 42)

With respect to the appointment of ISC members (who are presently selected by the PM in non-binding consultation with the Leader of the Opposition), the Government reviews two selection proposals involving Parliament, but does not indicate a preference. The Government also proposes to consider a potential increase of resources provided to the ISC. (page 43) Finally, the Government proposes that the ISC should be able to require information from UK agencies, subject to the veto of the relevant Secretary of State (currently, ISC requests for sensitive information related to sources, methods or operations can be declined by agency Heads). (page 44)

ii) The Commissioners (pages 44-46) and the Inspector-General model (pages 46, 47)

While the paper examines both the Intelligence Services Commissioner and the Interception of Communications Commissioner, it only forwards a proposal with respect to the Intelligence Services Commissioner. In addition to monitoring compliance by the agencies with the necessary

legal requirements in the exercise of intrusive powers, the Government proposes that the remit of the Intelligence Services Commissioner should be broadened to include the general responsibility for overseeing the effectiveness of operational policies. (page 45)

The paper also considers the adoption of an Inspector-General (IG) model for the UK (a single body that reviews all agencies, provides broad oversight, and has a more public role than that of a Commissioner). Negatively, the model is described as having the potential of becoming less independent than separate Commissioners; positively, it is regarded as being more transparent, coherent and credible. The Government is carefully considering the benefits and costs of adopting the model, with the possibility of an IG either subsuming the roles of the Commissioners; addressing oversight functions not covered by the Commissioners; or taking responsibility for all UK interception. (page 46)

Overall, the Government is concerned that any reform to the oversight system be balanced and minimize overlap (e.g. a parliamentary committee with a strong remit to examine operational policy would not be paired with an IG with the same power).

### **Assessment**

The central dilemma addressed by the *Green Paper* will be familiar to Canadian readers: how best to ensure the protection of information concerning sources, methods and investigations while making the best effort to provide a claimant with relevant information and evidence? While grappling with this dilemma, Her Majesty's Government has been compelled to withdraw evidence in civil cases where disclosure requirements risked exposure of sensitive information. The paper defends the use of Public Interest Immunity (PII) as the grounds for non-disclosure, but also notes the consequences of withdrawing evidence. In such cases the Government and security and intelligence agencies are denied an opportunity to defend themselves; judges are asked to render key decisions based on incomplete information; and both the Government and the taxpayer are exposed to potentially costly settlements when the case collapses. In part, the paper's proposals aim to minimize cases where this occurs.

An additional concern related to the practice of non-disclosure is the public perception that the Government's case is weak or unsubstantiated, or that the state is unwillingly to disclose information that might implicate it in unlawful or litigable activities (e.g. allegations that cooperation with another state led to the abuse of the claimant while in foreign detention). This perception contributes to a problem of credibility for UK agencies and the national security policy of the Government, particularly in the opinion of individuals in concerned demographics, the media, NGOs, and amongst segments of the legal and academic communities. As part of the credibility question, concerns are also voiced on how the agencies are held accountable for these and other decisions and activities, and if this oversight is itself credible.

Whether reasonable or not, these perceptions threaten to undermine key premises of national security policy and operations in a liberal democracy. Namely, national security is protected by covert operations that necessitate secrecy; related information can be legitimately kept secret from the public in the interest of national security; and, the state (Executive, Legislature, officials and the judiciary) will not abuse this trust and are accountable to Parliament and

citizens for decisions taken for the sake of national security. The *Green Paper* links the issue of the protection of sensitive information with these broader concerns by advancing proposals to increase the credibility of agency oversight.

As an example of how a liberal-democratic government in the Westminster parliamentary tradition addresses a national security policy challenge, the *Green Paper* is both interesting and informative. As expected, the state did not deviate from its primary responsibility to safeguard the public interest; preferring to make modest concessions to enhance the administration of justice for individuals that do not impair its capacity to investigate and deter threats. As such, the proposals will likely not have adverse effects on the UK agencies, apart from a potential for an additional drain on resources. Arguably, the most significant proposal in the report is the extension of CMPs. These types of proceedings are subject to criticism (as Canadians well know), and Amnesty International UK was quick to condemn the *Green Paper* and the expansion of CMPs as an entrenchment of secrecy within the judicial system. Nor is it probable that the UK Government will be applauded by critics in the NGO community for enhancing agency oversight, a process also constrained by secrecy. Given that the Government of Canada has mused about the possible establishment of a committee of Parliamentarians to review the activities of the Canadian S&I community, it is also of interest that the UK model is the subject of criticism and concern.

One lesson to be drawn from the UK exercise is that the liberal-democratic state is limited in how far it can reconcile the equally important imperatives of national security and procedural fairness in the administration of justice. As demonstrated by the initial reaction of Amnesty International UK, the public communications benefit can also be limited, particularly when interlocutors choose to frame the public debate in an adversarial manner.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

# Justice and Security Green Paper

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION



# Justice and Security Green Paper

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

Presented to Parliament by  
the Secretary of State for Justice  
by Command of Her Majesty  
October 2011



PROCESSED BY CRIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT /  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CRIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT /  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CRIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT /  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

© Crown copyright 2011

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit [www.nationalarchives.gov.uk/doc/open-government-licence/](http://www.nationalarchives.gov.uk/doc/open-government-licence/) or email [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk).

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to us at [justiceandsecurity@cabnet-office.x.gsi.gov.uk](mailto:justiceandsecurity@cabnet-office.x.gsi.gov.uk).

This publication is available for download at [www.official-documents.gov.uk](http://www.official-documents.gov.uk) and from <http://consultation.cabinetoffice.gov.uk/justiceandsecurity>

ISBN: 9780101819428

Printed in the UK for The Stationery Office Limited on behalf of the Controller of Her Majesty's Stationery Office.

Ref: 406595/1011

Printed on paper containing 75% recycled fibre content minimum.

# Contents

Foreword .....	vii
Executive Summary .....	xi
Key principles.....	xii
Areas of consultation.....	xiii
How to respond to the consultation .....	xvi
<b>Chapter 1: Background, recent developments and the case for change.....</b>	<b>3</b>
The twin imperatives of justice and security.....	3
Evolution of the principle of fairness in our justice system.....	5
Evolving role of the courts in national security.....	6
Existing mechanisms for handling sensitive material in civil courts – a summary .....	10
Recent developments – exacerbating the challenge.....	12
Closed material procedures and the Supreme Court: the case of <i>Al Rawi</i> .....	12
Cases struck out by courts .....	12
Providing a summary of the closed material to the excluded party, and the case of <i>Tariq</i> ...	13
Disclosure of sensitive material into foreign jurisdictions .....	14
Inquests involving sensitive material .....	15
Summary and the case for change.....	17
<b>Chapter 2: Sensitive material in civil proceedings: proposals and     consultation questions .....</b>	<b>21</b>
Enhancing procedural fairness .....	21
Proposal to expand CMPs to all civil judicial proceedings.....	21
CMPs and inquests.....	22
Improvements to the Special Advocate system.....	25
Clarifying the requirements for disclosure of damaging summaries of sensitive material: the ‘AF (No.3)’ principle or ‘gisting’.....	27

More active case-management powers for judges.....	28
Specialist court structures.....	29
The Investigatory Powers Tribunal.....	30
Safeguarding material.....	33
Enshrining PII in legislation.....	33
Addressing the challenge of court-ordered disclosure of sensitive material into foreign legal proceedings.....	35
<b>Chapter 3: Non-judicial oversight: proposals and consultation questions.....</b>	<b>39</b>
Ministerial responsibility and oversight.....	40
Independent parliamentary oversight.....	40
Procedural and practical improvements to the ISC.....	42
The Commissioners.....	44
The Inspector-General model.....	46
Ensuring a balanced system.....	47
<b>Appendix A: Secret intelligence, diplomacy and protecting the public.....</b>	<b>49</b>
<b>Appendix B: Public Interest Immunity.....</b>	<b>51</b>
<b>Appendix C: Closed material procedures.....</b>	<b>52</b>
<b>Appendix D: <i>AF (No.3)</i> and the challenges of providing summaries of sensitive material.....</b>	<b>54</b>
<b>Appendix E: Section 2(2) of the Security Services Act 1989 and sections 2(2) and 4(2) of the Intelligence Services Act 1994 ...</b>	<b>55</b>
<b>Appendix F: Further analysis on Special Advocates.....</b>	<b>56</b>
<b>Appendix G: Remit of the Commissioners.....</b>	<b>58</b>
<b>Appendix H: The Intelligence and Security Committee.....</b>	<b>59</b>

Appendix I: Possible model for an Inspector-General..... 60

Appendix J: Use of sensitive information in judicial proceedings:  
international comparisons ..... 61

Appendix K: Equality duties and impact assessments..... 65

Glossary ..... 67

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

## Foreword



The primary role of any government is to keep its citizens safe and free. That means both protecting them from harm and protecting their hard-won liberties. These two priorities should be mutually reinforcing – a safe, stable democracy is an ideal to which nations across the globe aspire.

In every democracy security and intelligence agencies play a central role in safeguarding this safety and stability. We owe an enormous debt of gratitude to these brave men and women who work tirelessly to protect us, particularly in response to the increased security challenges that this country has faced in the years following the attacks of 11 September 2001. They are a vital part of our nation's security and they must be a source of great national pride.

But this increase in intelligence activity has also led to greater scrutiny, including in the civil courts, which have heard increasing numbers of cases challenging Government decisions and actions in the national security sphere.

By their very nature such cases involve information which, under current rules, cannot be disclosed in a courtroom. This has rendered the UK justice system unable to pass judgment on these vital matters: cases either collapse, or are settled without a judge reaching any conclusion on the facts before them.

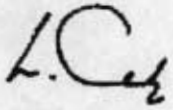
The Government is clear that this situation is wrong. It leaves the public with questions unanswered about serious allegations, it leaves the security and intelligence agencies unable to clear their name, and it leaves the claimant without a clear legal judgment on their case.

After over a year of careful consideration, we are bringing forward common-sense proposals which aim to:

- ♦ better equip our courts to pass judgment in cases involving sensitive information
- ♦ protect UK national security by preventing damaging disclosure of genuinely national security sensitive material
- ♦ modernise judicial, independent and parliamentary scrutiny of the security and intelligence agencies to improve public confidence that executive power is held fully to account.

As well as these important changes, the Prime Minister has already announced a package of measures aimed at restoring confidence in our security and intelligence agencies and allowing them to get on with the crucial job of keeping us safe. He announced the establishment of the Detainee Inquiry into whether the UK was involved in or aware of the improper treatment of detainees held by other countries. He published the consolidated guidance issued to intelligence officers and service personnel on engaging with detainees held overseas by third parties. He also announced the intention to reach a mediated settlement of the civil claims brought by former detainees of Guantanamo Bay because those claims could not be properly heard. This was achieved in November 2010. Combined with the proposals in this Paper which aim to improve our courts' ability to handle intelligence and other sensitive material, this represents a comprehensive package to address these difficult issues and to enable our security and intelligence agencies to get on with the vital task of keeping the UK safe.

These are matters of profound importance which go to the heart of our democratic values and our belief in human rights, justice and fairness. Inevitably, they are immensely complex and difficult – but we must not shy away from this debate. The prize is improved executive accountability, a court system equipped to handle sensitive material, and security and intelligence agencies that are able to get on with their job: a safer Britain, a fairer Britain.



Rt Hon Kenneth Clarke QC MP

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

# Executive Summary

## The challenge

1. The first duty of government is to safeguard our national security. In delivering this duty, the Government produces and receives sensitive information. This information must be protected appropriately, as failure to do so may compromise investigations, endanger lives and ultimately diminish our ability to keep the country safe.

2. Sensitive information can be used to prevent terrorist attacks, to disrupt serious crime networks and to inform decisions such as deportations and asset freezing. Such decisions are often challenged and reliable procedures are needed to allow such cases to be heard fairly, fully and safely in the courts. Some such procedures exist but the Government believes that there is scope to make improvements in response to recent court rulings.

3. Where the Government takes executive action and that action is subsequently challenged in the courts, there is ultimately the option – however damaging to national security – of dropping the action and withdrawing the case if we assess that the sensitive material will not be adequately protected due to disclosure requirements. In recent years, however, the Government has been called on to defend itself in increasing numbers of civil court proceedings initiated by others in which sensitive information is at the heart of the case and where withdrawing from the case without a potentially costly financial settlement is not an option.

4. The existing concept of Public Interest Immunity (PII)<sup>1</sup> enables sensitive material to be excluded from such cases but excluding key material means that the case cannot always be contested fairly for both sides. If too much material is excluded from court the Government may have little choice but to settle cases without a chance to defend itself.

5. In these and other such civil proceedings, judges are having to deliver judgments without being able to take into account key information. This weakens the UK's reputation as a free and fair democracy, respectful of human rights and the rule of law. It also means that security and intelligence agency activity risks not being properly considered through the justice system. Allowing this status quo to continue leaves open the increasing risk that the taxpayer will foot the bill to settle cases that the Government is prevented from defending. For the other parties in such proceedings too, this situation is clearly unsatisfactory. In exceptional cases material currently excluded under PII could benefit their case. And although parties may benefit financially or in other ways when a case is settled, they too – and the public as a whole – are left without a clear, independent ruling on the full facts of the case.

6. This Green Paper aims to respond to the challenges of how sensitive information is treated in the full range of civil proceedings. It will not look at the operation of criminal proceedings, nor the potential use of intercept as evidence.<sup>2</sup>

---

1 A fuller explanation of PII is given at Appendix B.

2 The Government is reviewing separately the use of intercept as evidence.

It seeks to find solutions that improve the current arrangements while upholding the Government's commitment to the rule of law. We urgently need a framework which will enable the courts to consider material which is too sensitive to be disclosed in open court, but which will also protect the fundamental elements that make up a fair hearing. These issues have recently been considered by the Supreme Court,<sup>3</sup> and this Green Paper seeks to build on these judgments.

7. At the same time, it is more important than ever that the public has confidence that the Government's national security work is robustly scrutinised, and that the bodies that undertake this work are as credible and effective as possible. So alongside the challenges arising in the courts, the Government has also taken this opportunity to examine the independent oversight arrangements for our security and intelligence agencies. A committee of Parliamentarians, two independent Commissioners and a specialist tribunal already exist and do a huge amount to ensure that the security and intelligence agencies are properly scrutinised and held to account. Yet the Government believes more can be done to modernise these arrangements and ensure that the oversight system as a whole is fit for the future role that is required.

8. Through this Green Paper, the Government wants to gather the best possible picture of the public's views on these issues in order to inform development of policies and legislative proposals.

9. The proposals outlined in this Paper apply across the UK in those policy areas where the UK Government's responsibilities extend across England, Northern Ireland, Scotland and Wales. Aspects of policy highlighted in the document will interact with matters which are devolved. The UK Government and the devolved administrations will continue to work closely together to ensure that the critically important objectives of the Green Paper are met. Respecting the judicial systems in Scotland and Northern Ireland, the

UK Government will use the period during the consultation to work with the devolved administrations on how best to effect changes in each jurisdiction.

## Key principles

10. In developing proposals to address these challenges we have been guided by the following key principles; that:

- ✦ rights to justice and fairness must be protected
- ✦ even in sensitive matters of national security, the Government is committed to transparency – and to demonstrating that we have no fear of scrutiny of even the most contentious public issues – and that it is in the public interest that such matters are fully scrutinised
- ✦ we must protect our sensitive sources, capabilities and techniques and our relationships with international partners, whose co-operation we rely on for our national security
- ✦ as much relevant material as possible should be considered by the courts in order that judgments are based on a complete picture and that justice is done more fully by reducing the number of actions that have to be settled or dropped
- ✦ Parliament should assist the courts by ensuring that appropriate mechanisms are available for handling these challenging cases and by clarifying when and how they can best be used
- ✦ reforms drawn from existing, tried and tested procedures will be easier to implement and more likely to succeed
- ✦ any proposals contain the necessary flexibility to be valid in any context or circumstance in which they may be required in the future
- ✦ effectiveness and credibility should be key considerations when considering possible improvements to the oversight arrangements of the security and intelligence agencies.

<sup>3</sup> See *Al Rawi v the Security Service* [2011] UKSC 34 and *Tarakh v Home Office* [2011] UKSC 35



## Areas of consultation

11. In considering the possible range of responses to these challenges, we have divided our proposals into three broad areas:

- ♦ Enhancing procedural fairness
- ♦ Safeguarding material
- ♦ Reform of intelligence oversight.

### Enhancing procedural fairness

12. Proposals in this section seek to **maximise** the amount of relevant material available for consideration in civil proceedings, while at the same time ensuring that sensitive material is afforded appropriate protection. The Government's objective is to ensure that proceedings are fair and full and to minimise the number of proceedings that cannot be tried because appropriate procedures do not exist to handle them.

#### Closed material procedures

13. There are already a number of specific legal contexts in which procedures are provided for in legislation so that sensitive material can be handled by the courts, most notably in the Special Immigration Appeals Commission. Such procedures have been shown to deliver procedural fairness and work effectively, and similar mechanisms are used internationally. **The Government proposes introducing legislation to make closed material procedures (CMPs) more widely available in civil proceedings for use in rare instances in which sensitive material is relevant to the case.**

*Question: How can we best ensure that closed material procedures support and enhance fairness for all parties?*

#### Closed material procedures in inquests

14. Extending CMPs for inquests involves particular challenges, because of the distinct nature of inquests from other civil proceedings, including the fact that inquests are conducted by a coroner

and sometimes with juries. **The Government seeks the views of the public on the applicability of CMPs to inquests.**

*Question: What is the best way to ensure that investigations into a death can take account of all relevant information, even where that information is sensitive, while supporting the involvement of jurors, family members and other properly interested persons?*

15. Inquests in Northern Ireland operate under a different framework.

*Question: Should any of the proposals for handling of sensitive inquests be applied to inquests in Northern Ireland?*

#### Special Advocates

16. The role of Special Advocates, who act in the interests of the party affected by the CMP, will be critical to the success of the proposed expansion of CMPs. The Government considers that there are some improvements that could be made and will ensure that further training and support are provided to Special Advocates. One area under particular consideration is the communication between the Special Advocate and the individual concerned after sensitive material is served (which requires the court's permission). The Government is giving consideration to reforms in this area to encourage Special Advocates to make use of existing procedures. An option could be for a 'Chinese wall' mechanism between government counsel and those clearing communications within an agency. The Government does not propose involving a separate judge in this process.

*Question: What is the best mechanism for facilitating Special Advocate communication with the individual concerned following service of closed material without jeopardising national security?*

### Gisting

17. This section considers the disclosure requirements developed in recent case law to provide the party affected by the CMP with a summary of some of the closed material, even where that is damaging to national security, and the merits of legislating to clarify the contexts in which provision of such a summary is and is not required (the so-called 'AF (No.3)'<sup>4</sup> or 'gisting' requirement).

*Question: If feasible, the Government sees a benefit in introducing legislation to clarify the contexts in which the 'AF (No.3)' 'gisting' requirement does not apply. In what types of legal cases should there be a presumption that the disclosure requirement set out in AF (No.3) does not apply?*

### Other proposals regarding procedures for handling sensitive material in civil proceedings

18. Consideration is given to:

- ♦ providing judges with more active case management powers in the pre-hearing phase to replicate best practice from more 'inquisitorial'-type proceedings (where proceedings are controlled and directed by the judge rather than the parties)
- ♦ establishing a 'specialist' court with appropriate safeguards to hear civil proceedings where sensitive material is relevant
- ♦ prospects for reform of the Investigatory Powers Tribunal (IPT).

*Question: At this stage, the Government does not see benefit in introducing a new system of greater active case management or a specialist court. However, are there benefits of a specialist court or active case management that we have not identified?*

*Question: The Government does not see benefit in making any change to the remit of the Investigatory Powers Tribunal. Are there any possible changes to its operation, either discussed here or not, that should be considered?*

### Safeguarding material

19. Another approach to resolving the challenges outlined above would be to reinforce existing mechanisms to prevent harmful disclosure of sensitive information.

#### Enshrining Public Interest Immunity (PII) in legislation

20. Consideration is given to enshrining the common law principle of PII in legislation and to include a presumption against the disclosure of categories of sensitive material, such as that held by the Government but owned and originated by an international partner. However, in order to conform with our domestic and European obligations, any statutory presumption would likely have to be rebuttable, so there would be little advance on the current system. If the reforms to extend CMPs are introduced, PII would have a reduced role, in any case. **The Government does not propose to pursue this option.**

*Question: In civil cases where sensitive material is relevant and where closed material procedures are not available, what is the best mechanism for ensuring that such cases can be tried fairly without undermining the crucial responsibility of the state to protect the public?*

#### Court-ordered disclosure where the Government is not a primary party

21. This relates to a special category of civil claim – where a claimant seeks disclosure of sensitive material to assist them in another set of proceedings, usually abroad. A CMP is not

4 Secretary of State for the Home Department v AF [2009] UKHL 28

sufficient to protect the material, because it is actual disclosure of that sensitive material that is sought. **The Government proposes to limit the role of the courts in cases in which individuals are seeking disclosure of sensitive material, where the Government is not otherwise a party, particularly into foreign legal proceedings over which we have no control (via so-called 'Norwich Pharmacal' applications).** This section considers several options to reduce the potentially harmful impact of such court-ordered disclosure, including introducing legislation to clarify that Norwich Pharmacal principles should not apply where disclosure of the material in question would cause damage to the public interest.

**Question: What role should UK courts play in determining the requirement for disclosure of sensitive material, especially for the purposes of proceedings overseas?**

## Reform of intelligence oversight

22. Proposals in this section examine ways in which the existing independent and parliamentary oversight bodies may be made more effective, and be seen to be more effective, thus increasing public confidence. The Government is keen to hear views on the appropriate balance between independent and parliamentary oversight. The key overarching consultation questions on oversight reform are as follows.

**Question: What combination of existing or reformed arrangements can best ensure credible, effective and flexible independent oversight of the activities of the intelligence community in order to meet the national security challenges of today and of the future?**

**Question: With the aim of achieving the right balance in the intelligence oversight system overall, what is the right emphasis between reform of parliamentary oversight and other independent oversight?**

## Parliamentary oversight

### *The Intelligence and Security Committee*

23. The Intelligence and Security Committee (ISC) provides parliamentary oversight of the security and intelligence agencies. The Government supports a number of proposals to modernise the ISC and change its status, remit and powers. A key question for reform is whether the status of the ISC can be changed, to strengthen its links to Parliament. The Government proposes, in line with the ISC's own proposals, that it becomes a statutory Committee of Parliament. The Government is also committed to working with the ISC to provide public evidence sessions and agrees with the ISC's proposal to have the power to require information from the security and intelligence agencies, with a veto resting with the Secretary of State.

**Question: What changes to the ISC could best improve the effectiveness and credibility of the Committee in overseeing the Government's intelligence activities?**

## Independent oversight

### *The Commissioners*

24. Independent oversight of the security and intelligence agencies is also provided by the Intelligence Services Commissioner and the Interception of Communications Commissioner. In order to improve their effectiveness and credibility, this section examines whether to broaden their remit and outlines changes already taking place to increase the public profile of the Commissioners. The potential benefits of creating an Inspector-General are also examined.

**Question: What changes to the Commissioners' existing remit can best enhance the valuable role they play in intelligence oversight and ensure that their role will continue to be effective for the future? How can their role be made more public facing?**

### *An Inspector-General*

25. An alternative approach for independent oversight would be for an Inspector-General, which concentrates more oversight functions in one body. Importing such a system into the UK would require an overhaul of the Commissioner arrangements and would need careful management to ensure that its remit did not overlap with the ISC. The Government is considering whether the benefits of such a system would outweigh the costs. A number of approaches could be taken.

**Question: Are more far-reaching intelligence oversight reform proposals preferable, for instance through the creation of an Inspector-General?**

### How to respond to the consultation

26. This is a public consultation to which anyone with an interest may respond. The Government invites the contribution of evidence, ideas and recommendations in response to the questions posed in this Green Paper.

Responses should be sent to [justiceandsecurity@cabinet-office.x.gsi.gov.uk](mailto:justiceandsecurity@cabinet-office.x.gsi.gov.uk) by Friday 6 January 2012.

Responses can also be filed online on the website <http://consultation.cabinetoffice.gov.uk/justiceandsecurity>

Alternatively, responses can be sent to the following postal address: Justice and Security Consultation, Cabinet Office Room 335, 3rd Floor, 70 Whitehall, London SW1A 2AS.

# Chapter 1

## Background, recent developments and the case for change

### The twin imperatives of justice and security

1.1 When the Coalition came into government in May 2010 it stated that its first duty was to safeguard national security while at the same time affirming a commitment to be strong in the defence of our freedoms.<sup>1</sup> The Coalition's Programme for Government was based on the three core principles of freedom, fairness and responsibility and the Government stated that it believes that more needs to be done to ensure fairness in the justice system.

1.2 The Government recognises that preserving a strong and independent judiciary is one of the most effective safeguards of the freedom, rights and liberties of its people. The ability to effectively vindicate one's rights through the justice system is a vital element in a modern democracy. It ensures that justice, in its broadest sense, can be done, and it provides an essential check on executive action.

1.3 The Government has a range of capabilities for providing security to those within its jurisdiction, for keeping its people safe and to enable vital institutions such as the courts to continue to function properly. These include the police and law enforcement agencies, the armed forces, the diplomatic service and the security and intelligence agencies (the Secret Intelligence Service or MI6, the Security Service or MI5 and the Government Communications Headquarters or GCHQ; collectively the Agencies). The Agencies, together

with the intelligence gathering arms of the armed forces and law enforcement agencies, provide a secret, or covert, capability which is an essential element in the Government's national security capability. Secret intelligence allows the Government to disrupt individuals, networks and events that pose a threat to national security and the economic well-being of the country.

1.4 Appendix A on page 49 contains further explanation of the types of government business that generate sensitive material.

1.5 As with all public bodies, it is essential that the Agencies are subject to effective judicial and non-judicial scrutiny in order that the public has confidence that they are working lawfully, effectively and efficiently for the good of the public.

1.6 In considering the role of the courts and parliamentary and independent oversight bodies in scrutinising matters of national security, we must strike a balance between the transparency that accountability normally entails, and the secrecy that security demands. This Paper will examine this balance and make proposals to ensure that oversight mechanisms – both judicial and non-judicial – are relevant and effective in the modern era. Excessively strong national security structures may make us safer but not freer, and security structures that are too weak put at risk the values, freedom and way of life that we all both hold dear and take for granted.

---

<sup>1</sup> *The Coalition: our programme for government (2010)*, pages 7 and 11

### Recent secret intelligence successes

- Secret intelligence can be used to prevent individuals from engaging in terrorist-related activities, which of course may save lives. In 2006, a 'liquid bomb' plot was foiled; this was an attempt to launch simultaneous suicide attacks against multiple mid-flight transatlantic airliners, which would have resulted in thousands of fatalities.
- On 29 October 2010, two explosive devices concealed in air freight were discovered and intercepted following the receipt of specific intelligence. One device, concealed in a printer, was found at East Midlands Airport on an inbound flight en route from Yemen to Chicago that had transited through Cologne. The other device was intercepted at Dubai International Airport, also en route from Yemen to Chicago. Both devices were probably intended to detonate over the Atlantic or the eastern seaboard of the United States. They may have brought down the aircraft.
- Through secret intelligence we can seek to mitigate the risk from states who seek to obtain weapons of mass destruction, whether nuclear, chemical or biological, through identifying ways to slow down or remove the access of such states to essential equipment and technology. The recent discovery of Iran's secret nuclear facility at Qom was one such intelligence success.
- In military conflicts, secret intelligence can be decisive, including in counter-insurgency situations. Tactical (short-term) intelligence, for example, can provide vital information for military operations, leading to gains on the battlefield, potentially saving the lives of the UK's service personnel. Strategic (long-term) intelligence can help plan for the political way forward (such as in Afghanistan).
- Secret intelligence can help to thwart the continuing threat from foreign espionage. This was demonstrated recently by the discovery and arrest of a group of Russian 'illegals' in the USA and Cyprus in 2010, of whom one had significant UK ties. Intelligence enables the Government to guard against such threats and protect the UK's interests, preventing hostile states from gaining sensitive information that could damage the UK's economy, reduce the UK's advantage in advanced military capabilities and damage the effectiveness of the UK's diplomacy.
- Secret intelligence plays a key role in the fight against serious and organised crime. For example:
  - Surveillance by the Serious Organised Crime Agency (SOCA) on a print business in the UK resulted in a total of more than 34 years' imprisonment for five organised crime group members convicted of counterfeiting £20 banknotes worth millions of pounds. To date, banknotes with a face value of more than £17.5 million believed to be linked to the gang have been removed from circulation.
  - In July 2011, secret intelligence led to the seizure of 1.2 tonnes of high-purity (90%) cocaine in Southampton and the subsequent surveillance and arrest of six members of the organised crime group responsible in the Netherlands.
- Secret intelligence can provide information on the intentions and capability of hostile state or non-state actors to launch cyber attacks against UK networks. Such attacks may be aimed at stealing information or damaging the integrity of the networks themselves. Secret intelligence has a role in detecting and preventing such attacks.

## Evolution of the principle of fairness in our justice system

1.7 Protections to ensure procedural fairness and fair trials in the justice system have evolved gradually over the centuries. The rules of natural justice have developed over time, one of which is the right to know the opposing case. What this means will vary depending on the circumstances.

1.8 Additionally and linked to the rules of natural justice is the principle that justice should not only be done, but must also be seen to be done.<sup>2</sup> A number of procedural requirements and rules arise out of this principle: for example, the requirement that judges must give reasons for their decisions that court hearings should be held in public and that the press should be free to report on court proceedings. Taken together, these requirements help achieve the aim of open justice. Again, these are not absolute requirements that allow no exceptions.

1.9 There are a number of limited but well-recognised exceptions to the open justice principle which do not infringe on the requirement that hearings should be fair. These are set out in the Civil Procedure Rules.<sup>3</sup> A hearing, or any part of it, may be in private in certain circumstances. For example, a private hearing may be necessary to protect the interests of any child<sup>4</sup> or if the court considers it necessary in the interests of justice<sup>5</sup> or of national security.<sup>6</sup> Similarly, it may be compatible with the right to a fair and public hearing in Article 6 of the European Convention on Human Rights (ECHR) for hearings to be held in private or for information to be withheld from parties, as long as there are sufficient procedural safeguards.

### Article 6 and the right to a fair trial

Article 6 of the ECHR requires that in proceedings determining a person's civil rights, the person is entitled to a fair hearing. The requirements of a fair hearing will be more onerous – approaching those required for criminal proceedings – in civil cases that determine a significant matter such as the claimant's liberty. The principle is that the protections provided in the proceedings should be commensurate with the gravity of the potential consequences on the individual concerned.

Article 6 requires that hearings should normally be held in public, although exceptions are permitted on grounds such as national security.<sup>7</sup> Under Article 6, relevant evidence should generally be disclosed to the parties to civil proceedings.<sup>8</sup> But this right is not absolute, and limits on disclosure may be justified, for example in the interests of national security in order to protect the public from harm.<sup>9</sup>

1.10 The British Government is committed to open justice. However, in justice, as in other areas, the benefits of transparency have to be balanced against important imperatives, such as national security. In certain instances, to hear a case in public or disclose information to the other party would be to endanger national security, and to withdraw from or settle the case (which may be the only alternatives) could also endanger national

2 *R v Sussex Justices Ex parte McCarthy* [1924] 1 K.B. 256 as per Lord Hewitt CJ: 'it is not merely of some importance, but is of fundamental importance that justice should not only be done, but should manifestly and undoubtedly be seen to be done.'

3 The Civil Procedure Rules (CPR) in Scotland and Northern Ireland are also based on the same principles.

4 CPR Rule 39.2(3)(d)

5 CPR Rule 39.2(3)(g)

6 CPR Rule 39.2(3)(b)

7 *Kennedy v UK* (2011) 52 EHRR 4, at [188]

8 E.g. *Martinie v France*, App. No. 58675/00, judgment of 12 April 2006, at [45]-[50]; *Hudakova v Slovakia*, App. No. 23083/05, judgment of 27 April 2010, at [25]-[32]

9 *Jasper v UK* (2000) 30 EHRR 441, at [52]; *A and Others v UK* (2009) 49 EHRR 29, at [205]; *Kennedy v UK* (2011) 52 EHRR 4, at [184].

security or public safety as well as not being in the interests of justice overall.

1.11 As we shall see in the following sections of this Paper, the law has developed significantly in recent years in response to the question of how to facilitate appropriate handling of relevant sensitive material in civil court proceedings in a way that is consistent with well-developed principles of natural justice and fairness. But in a number of respects the law remains uncertain.

1.12 The Government believes that it is now time to bring clarity to this area of the law. The proposals aim both to safeguard national security and to establish a durable, sustainable and just framework by which sensitive material may be handled securely and effectively in civil proceedings. The Government's intention is that a Minister will be able to make a statement of compatibility in relation to any Bill which implements the proposals flowing from this consultation document in accordance with section 19(1)(a) of the Human Rights Act 1998.

### Evolving role of the courts in national security

1.13 It is long established in the UK, and a fundamental pillar of the rule of law, that the courts are independent adjudicators to which the executive powers of government must be answerable.

1.14 One form of scrutiny of the compliance of governmental and public bodies with the law is judicial review. In a judicial review a judge will seek to determine whether a body has exercised its powers lawfully. Judicial review is a flexible tool that allows differing degrees of intensity of scrutiny depending on the circumstances and the impact of the decision on the individual concerned.

1.15 Recourse to judicial review has increased significantly in recent decades, from 160 applications in 1974 to 4,539 in 1998.<sup>10</sup> By 2010 the number of applications had reached 10,548.<sup>11</sup>

1.16 Coinciding with this period of increased development of judicial review were the two Acts of Parliament that placed the Agencies on the statute book – the Security Service Act 1989 and the Intelligence Services Act 1994. Furthermore, the Regulation of Investigatory Powers Act 2000 (RIPA) regulates the powers of public bodies, including the Agencies, to carry out surveillance and covers the interception of communications. With the Agencies underpinned by statute, their activities formally regulated and overseen, and against the backdrop of an increased public recourse to judicial review, judicial and non-judicial scrutiny of the Agencies became more commonplace.

1.17 The Agencies have been affected by an increasing number of court cases over the past decade. The increased recourse to judicial review, and increased awareness of the importance of national security in the years after the attacks of 11 September 2001, were drivers for this change. In addition, the unprecedentedly high level of threat against the UK from both home and abroad meant that the Agencies were required to act faster, co-operate with more international liaison partners and investigate more threats in order to protect the public. Some of the operational activities of the Agencies during this period have recently been, and continue to be, scrutinised in the courts, through civil damages claims filed by former Guantanamo detainees, through public inquests (such as the recently concluded inquests into the 7 July 2005 bombings), through appeals against decisions relating to Control Orders and immigration decisions, or through judicial review of Government decisions in the national security context. By way of illustration, in the first 90 years of the Security Service's existence, no case impacting directly on that Service's work reached the House of Lords. In the last ten years there have been 14 such cases in the House of Lords or Supreme Court. All three Agencies have been involved in many more cases heard in the lower courts.

10 Treasury Solicitor (2000), *The Judge Over Your Shoulder: a guide to judicial review for UK government administrators*, 3rd edition

11 Source: [www.judiciary.gov.uk](http://www.judiciary.gov.uk)



### **Criminal vs Civil: Why criminal proceedings are out of scope for this Paper**

Civil and criminal proceedings in England and Wales are fundamentally different. In **civil** cases, the courts adjudicate on disputes between parties under the civil law. In **criminal** cases, it is usually the state which prosecutes individuals for the commission of criminal offences; where defendants are convicted, they face criminal sanctions including imprisonment. Due to the understandably more onerous requirements of the right to a fair trial in criminal cases, the rules concerning the use and protection of sensitive evidence are different to those in civil cases.

**Criminal proceedings** have the strictest requirements under Article 6 of the ECHR regarding the disclosure of sensitive material. Long-standing procedures, generally supported by all parties, are in place:

- The evidence that the prosecutor uses in court to secure a conviction is never withheld from the accused.
- The prosecutor is required to disclose to the accused all relevant material obtained in an investigation (whether or not it is admissible as evidence) that might reasonably be considered capable of undermining the prosecution case or of assisting the case for the accused – this is known as the 'unused material'.
- If the prosecutor considers that any of this 'unused material' is too sensitive to be disclosed, in order to continue the prosecution, the prosecutor must apply to the court for permission not to disclose the material. Material may be sensitive if it relates to national security, to police informants or to a child's social services records, for example. This involves a Public Interest Immunity or PII application – the same mechanism that exists in civil proceedings and **is discussed fully elsewhere in this Paper.**
- The court can, however, decide to overturn the PII certificate and order disclosure; the prosecutor will have a right of appeal in certain cases and – clearly if the risk resulting from disclosure is too great – ultimately the prosecutor has the discretion to withdraw the prosecution. This will result in the acquittal of the accused, but the sensitive material will not be disclosed.

In Scotland, provisions relating to disclosure of material in a PII application are set out in the Criminal and Licensing (Scotland) Act 2010.

In **civil** claims, as HMG is a defendant, there is no possibility of withdrawing from the case, so the ability to protect sensitive material is entirely dependent on PII claims.

1.18 Given this increased volume of court cases, the lack of an effective framework in which the courts can securely consider sensitive material presents a very real challenge in proceedings in which sensitive material is centrally relevant. The Government has strained key international relationships and risked compromise of vital sources and techniques in no fewer than seven court cases in which the applicants sought sensitive UK Government-held but very often foreign government-originated information for disclosure into foreign legal proceedings; and the

Government has had to reach expensive out-of-court settlements with former Guantanamo detainees because of a lack of an appropriate framework in which civil damages claims involving sensitive material could be heard.

1.19 In addition, in certain immigration cases, in particular when taking a decision to exclude from the UK on national security grounds an individual who holds no current immigration status, the only form of legal challenge available to the individual is judicial review. The courts had recently approved

the use of a closed material procedure (CMP)<sup>12</sup> in judicial reviews<sup>13</sup> but this is now subject to the decision in *Al Rawi*<sup>14</sup> (see paragraph 1.32 for detail). The absence of CMPs in judicial review may make the defence of the decision extremely difficult, particularly in cases where the majority of the case consists of sensitive material. The court may conclude that it needs to consider the full facts of the case in order to come to an informed decision and that without that material the exclusion decision cannot stand. This may result in the Secretary of State being unable to exclude individuals from the UK that they consider to be a threat to national security because they cannot defend the actions in court.

1.20 In contrast, in the very specific legal contexts in which effective mechanisms for considering sensitive material do exist, most notably in the Special Immigration Appeals Commission (SIAC),<sup>15</sup> the Government is successfully delivering its national security requirements while also fulfilling its legal and human rights obligations. SIAC has been used in around 70 cases since December 2001, of whom 10 individuals have been deported and another 11 have left voluntarily. Some of those 70 have been subject to deprivation of citizenship proceedings, some to immigration decisions relating to an exclusion from the UK, and a number of others have been detained or put on strict bail for a period of time, reducing their ability to engage in terrorist or criminal activity. They may also still be facing deportation as their cases progress through the courts.

1.21 The UK's counter-terrorism strategy, CONTEST, also makes clear that we want to 'ensure that judicial proceedings in this country can better handle sensitive and secret material

to serve the interests of both justice and national security'.<sup>16</sup> This is a key objective in our counter-terrorism strategy and is consistent with our Pursue objective: that our counter-terrorism work is **effective, proportionate and consistent with our commitment to human rights**.

1.22 There is the further challenge of ensuring that we, the UK Government, honour our understandings with foreign governments by safeguarding sensitive material that they have shared with us (see 'The Control Principle' on the next page for more detail). In the aftermath of the UK court-ordered release of sensitive US intelligence material in *Binyam Mohamed*<sup>17</sup> (see second box on the next page for detail), the UK Government has received clear signals that if we are unable to safeguard material shared by foreign partners, then we can expect the depth and breadth of sensitive material shared with us to reduce significantly. There is no suggestion that key 'threat to life' information would not be shared, but there is already evidence that the flow of sensitive material has been affected. The risk is that such material withheld by a foreign partner might, when pieced together with other intelligence material in the possession of the Government, provide the critical 'piece of the jigsaw' that would allow a threat to be contained, or a terrorist to be brought to justice. The fullest possible exchange of sensitive intelligence material between the UK and its foreign partners is critical to the UK's national security.

12 A fuller explanation of CMPs is given at Appendix C.

13 *R(AHK) v Secretary of State for the Home Department* [2009] EWCA Civ 287

14 *Al Rawi v Security Service* [2011] UKSC 34

15 Established under the Special Immigration Appeals Commission Act 1997

16 *CONTEST: The United Kingdom's strategy for countering terrorism* (2011), page 10, paragraph 1.17

17 *R. (Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 65

### **The Control Principle**

To help to keep the UK as safe as possible, we need to receive secrets from other countries. Secret intelligence gathered by foreign governments and shared with us on a strictly confidential basis represents a significant proportion of all the information that we gather on terrorists, organised criminals and others seeking to harm our national security. Analysing the foreign material in conjunction with our own domestically generated intelligence information allows us to construct as full and detailed a picture as possible of the threats against us so that we may determine how best to thwart them. Any reduction in the quality and quantity of intelligence that overseas intelligence partners share with us would materially impede our intelligence community's ability to do what is asked of them in protecting the security interests of the United Kingdom.

In all intelligence exchanges it is essential that the originator of the material remains in control of its handling and dissemination. Only the originator can fully understand the sensitivities around the sourcing of the material and the potential for the sources, techniques and capabilities to be compromised by injudicious handling. We expect our intelligence partners to protect our material when we share it with them, and we must be able to deliver the same protection of their material. Confidence built up over many years can all too quickly be undermined. That is why, if the trust of the UK's foreign 'liaison' partners is to be maintained, there should be no disclosure of the content or fact of the intelligence exchange with them without their consent. This is known as the **Control Principle**.

### ***Binyam Mohamed* and court-ordered disclosure challenges**

In May 2008, *Binyam Mohamed* brought judicial review proceedings against the Foreign Secretary. Under 'Norwich Pharmacal' principles (see the box on page 15), he sought disclosure of information and documents necessary to assist his defence in his trial before a US military commission and, in particular, to show that the prosecution case consisted of evidence obtained through torture.

The Foreign Secretary said that to disclose material that has been passed to the UK on intelligence channels would breach the Control Principle. He argued, therefore, that the court should not order disclosure in this case.

Disclosure issues in the *Binyam Mohamed* judicial review case were resolved in part by disclosure of certain documents (with redactions) by the US authorities to *Binyam Mohamed*'s security-cleared US legal team. In the meantime the Foreign Secretary continued to seek PII protection of other information contained in seven paragraphs of one of the UK court's closed judgments in the judicial review proceedings (the 'seven paragraphs') on the grounds that to disclose it would breach the Control Principle, and that such a breach would be damaging to intelligence sharing and thereby national security. The seven paragraphs summarised material passed to the UK on intelligence channels. The legal issue about the public disclosure of the seven paragraphs reached the UK Court of Appeal some time after *Binyam Mohamed* had returned to the UK. By the time that court handed down its judgment, a court in the US had made findings of fact directly relevant to the content of the US reporting in the seven paragraphs. This US court finding appears to have been a critical factor in the Court of Appeal's decision not to uphold the Foreign Secretary's claim for PII. The US Government continues to assert that the relevant information is classified, contrary to the Court of Appeal decision.

*Mohamed* went on to join other former detainees in a civil claim for damages against the UK Government, alleging, among other things, complicity in his rendition, detention and torture. In November 2010, the parties agreed a mediated settlement, the terms of which remain confidential. The Government made no admission as to liability.

## Existing mechanisms for handling sensitive material in civil courts – a summary

1.23 Common law principles have developed to ensure that a case involving sensitive material can proceed as fairly as possible. The traditional common law tool in these cases is PII. For more detail, see Appendix B.

1.24 The courts have long recognised that evidence, while relevant to the issues between the parties in a case, must be **excluded** if the public interest in withholding the information outweighs the public interest in disclosing it. This involves the court balancing competing aspects of the public interest: the public interest in preventing harm to national security and the public interest in the administration of justice, for example.

1.25 The areas of public interest that may be protected by PII include: national security, international relations and the prevention or detection of crime. The categories of PII are not fixed.<sup>18</sup> However, the courts will not recognise new categories of immunity without clear and compelling evidence.<sup>19</sup>

1.26 In addition to the obligation on the Crown to raise PII where relevant, the Heads of the Agencies are under a statutory duty to ensure that there are arrangements to secure that no information is disclosed by the Agencies except insofar as it is provided for in statute. For more detail on this statutory duty, see Appendix E.

1.27 More recently and for very specific legal contexts, Parliament has made statutory provision

for a mechanism through which sensitive material can be handled by the courts. These are known as closed material procedures (CMPs), and were first established to facilitate the hearing of national security sensitive deportation cases through the SIAC.<sup>20</sup> A number of other countries use CMPs in civil legal proceedings. For more detail, see Appendix J.

1.28 A CMP is a procedure in which relevant material in a case, the disclosure of which would be contrary to the public interest, is neither openly disclosed to the other party or its legal team nor excluded from consideration but instead disclosed to the court and to Special Advocates appointed by the Attorney General<sup>21</sup> to represent the other party's interests. For more detail, see Appendix C. **A CMP will represent a part, possibly only a small part, of the overall case, the rest of which will be heard in open court.**

1.29 A CMP is capable of satisfying the requirements of the ECHR.<sup>22</sup> Under Article 6, there may be restrictions on the right to a fully adversarial procedure where strictly necessary in the light of a strong countervailing public interest, such as national security.<sup>23</sup>

1.30 A CMP enables the court to take into account relevant material that might otherwise be excluded from consideration altogether by the operation of PII. A CMP is a mechanism for seeking to reconcile the public interest in the administration of justice and the public interest in safeguarding national security.

18 Lord Hailsham remarked in *D v NSPCC* [1978] AC 171 that 'the categories of public interest are not closed and must alter from time to time whether by restriction or extension as social conditions and social legislation develop'.

19 *R v Chief Constable, West Midlands ex p Wiley* [1995] 1 AC 274

20 Established through the Special Immigration Appeals Commission Act 1997.

21 In Scotland appointed by the Advocate General.

22 *A and Others v UK* (2009) 49 EHRR 29; *Kennedy v UK* (2011) 52 EHRR 4; *Chahal v UK* (1997) 23 EHRR 413, at [131]; *Al-Nashif v Bulgaria* (2003) 36 EHRR 37, at [95]-[97]; *Secretary of State for the Home Department v AF (No. 3)* [2009] UKHL 28; *Tariq v Home Office* [2011] UKSC 35

23 *Kennedy v UK* (2011) 52 EHRR 4, at [184]

### Intercept as evidence: a separate challenge and a separate Government project

Intercept as evidence (IAE) is the proposed use of intercept material (for example telephone calls, emails and other internet communications) obtained under a RIPA<sup>24</sup> warrant as evidence in criminal proceedings.

Both the Green Paper and work on IAE reflect the Government's commitment to justice, openness and transparency and its desire that, wherever possible, evidence is brought before the courts. However, as made clear when it was announced, the Green Paper is not the appropriate means for addressing the Government's commitment to seeking a practical way of adducing intercept evidence in court. Although some of the issues may appear related, in practice the topics are clearly distinct. Seeking to group them would complicate and delay progress rather than expedite it. Importantly:

- First, the Green Paper is centred on civil proceedings, addressing specific issues raised by recent court judgments. In contrast, work on IAE is centred on the practicalities of introducing its use across serious criminal proceedings. Intercept material can already be adduced in certain civil proceedings, such as SIAC and Proscribed Organisations Appeal Commission cases.
- Second, the Green Paper is centred on the issue of protecting sensitive material. While this must also form an essential feature of any viable IAE regime, the requirements of Article 6 of the ECHR are different – and more demanding – in the criminal than the civil sphere. So bespoke solutions need in any event to be developed for both circumstances.
- Finally, the issues to be addressed in developing a legally compliant and operationally practical approach to IAE go much wider than protecting sensitive material alone – essential though this is.

Reflecting this, work on IAE continues to be overseen by the cross-party Advisory Group of Privy Counsellors.

### Recent developments – exacerbating the challenge

1.31 Previous sections have described in general terms the challenges to the fair administration of justice in the national security sphere. In this section we examine in some more detail the specifics of the challenge and the particular cases and contexts that have given rise to the most notable challenges to the administration of justice, the current lack of clarity in terms of the operations of the current system, and the biggest concerns in terms of the safeguarding of our most sensitive material.

#### Closed material procedures and the Supreme Court: the case of *Al Rawi*

1.32 In the case of *Al Rawi v Security Service*,<sup>25</sup> the Supreme Court was asked to consider whether the court has the power to order a CMP for the whole or part of a civil claim for damages. The issue arose in a civil claim for damages brought by former detainees in Guantanamo Bay who alleged that the UK Government was complicit in their detention and ill treatment by foreign authorities. In their defence the defendants wished to rely on material the disclosure of which would cause harm to the public interest and asked the court to determine the preliminary issue of whether a court could adopt a CMP in such a claim. A successful claim of PII in relation to this material would have led to its exclusion but would have made progression of the case more difficult. The defendants argued that they should be able to defend themselves by relying on important evidence in a CMP. Although the underlying claim was settled on confidential terms, the Supreme Court continued to hear the appeal on this important point of principle.

1.33 The majority of the Supreme Court held that in the absence of statutory authority, it was not open to the court to adopt a CMP in such a claim. Many of the judgments took the view that provision for a CMP is a matter for Parliament and not the courts. Lord Clarke, for example, stated that:

*It would be better for the problems which arise in this class of case to be dealt with by Parliament.*<sup>26</sup>

The Supreme Court acknowledged that the absence of a CMP could lead to a claim being untriable and struck out, as was the case in *Carnduff v Rock*<sup>27</sup> (see following paragraphs).

#### Cases struck out by courts

1.34 In *Carnduff v Rock*<sup>28</sup> a majority of the Court of Appeal found that that case could not be litigated consistently with the public interest and that it should be struck out. The determination of the claim would have required the disclosure of information that was sensitive, such as the operational methods used by police and how they made use of informers' information. The court would have required this information in order to investigate and adjudicate upon the claim. Disclosure of this information was not in the public interest and thus the case was not allowed to proceed.

1.35 The claimant complained to the European Court of Human Rights (ECtHR), alleging a breach of Article 6, but his complaint was rejected as unfounded.<sup>29</sup> The ECtHR found that the 'strike out' did not amount to preventing Mr Carnduff from having access to the court. A key part of their reasoning is that the case was only struck out after full oral, reasoned argument before the Court of Appeal, during which the applicant was legally represented.

25 [2011] UKSC 34

26 At [162]; see also Lord Dyson at [44] and [48], Lord Hope at [74] and Lord Phillips at [192], who all comment along similar lines.

27 [2001] EWCA Civ 680

28 *Carnduff v Rock and another* [2001] EWCA Civ 680 involved a claim by a registered police informer. He sought to recover payment for information that he supplied to West Midlands Police. The police denied any contractual liability to make the payments or that the information provided by the claimant had led to the arrests or prosecutions which the claimant suggested.

29 *Carnduff v United Kingdom* (App. No. 18905/02) (unreported) 10 February 2004

1.36 This was a decision that was reached on the particular facts and pleadings of the case. The Supreme Court in *Al Rawi* did acknowledge that there could be cases that could not be tried at all consistent with the public interest.<sup>30</sup> Although the approach taken in *Carnduff* remains an option that is open to the courts in England and Wales, **the Government favours having as many cases as possible tried fully and fairly.** To this end, the availability of a CMP in cases involving sensitive information would allow sensitive information to be considered by a court in a manner that is consistent with the public interest. There are cases in which there are competing public interests, such as the public interest in achieving justice for both parties, and the public interest in maintaining the operational effectiveness of the Agencies. Where they are currently available, CMPs allow these competing aspects of the public interest to be reconciled.

#### Providing a summary of the closed material to the excluded party, and the case of *Tariq*

1.37 The Government has always sought to ensure that at the outset of the case the excluded party in a CMP is given as much material as possible, including summaries of the sensitive case against them, subject only to public interest concerns related to national security. (This process is often abbreviated, and referred to from now on in this Paper as 'gisting'.) However, in recent judgments the courts have decided that in cases in which the liberty of the individual is to some extent at stake<sup>31</sup> (although the precise extent of this has yet to be determined – see paragraph 1.39 below) Article 6 of the ECHR requires that excluded parties in CMPs need to be provided with a summary of the main elements of the intelligence case against them, even where the gist will cause damage to national security through the

disclosure of sensitive material. See Appendix D for a summary of a key case in this area.

1.38 The Secretary of State will in any event provide as complete a gist of the intelligence case to the excluded party in the CMP as is possible within the constraints of national security. However, by virtue of having to provide a summary of the case against the individual that includes the disclosure of information damaging to national security, the Secretary of State sometimes faces the significant risk that, for example, the source or technique used to obtain the information about the individual might become known to the individual and their legal representatives, with resultant potential harm to the public interest including national security. Not providing the required gist in such cases may mean forfeiting the action or order against the individual, with a similarly harmful impact on the public interest or not allowing the Government to defend itself in an action brought against it.

1.39 The case law so far has not clearly established the circumstances in which Article 6 requires gisting. In the case of *Tariq v Home Office* (2011),<sup>32</sup> the Supreme Court had recently to determine whether there was a requirement to provide a gist to an individual who had brought a claim of race and religious discrimination before the Employment Tribunal. The claim related to a decision to withdraw the claimant's security clearance and suspend him from duty following the consideration of national security sensitive information. The majority of the Supreme Court<sup>33</sup> found that gisting was not required in every context in which Article 6 was engaged and that it was not required in a context related to national security vetting such as in *Tariq*. Lord Hope expressed this point in the following way at paragraph 83:

30 See Lord Dyson at [15], Lord Brown at [86], Lord Mance at [108] and Lord Clarke at [157].

31 This follows a ruling in the ECtHR, *A and Others v UK* (2009) 49 EHRR 29, which was built upon by the House of Lords in *Secretary of State for the Home Department v AF* (No.3) [2009] UKHL 28 – for more detail on both these cases, see Appendix D.

32 *Tariq v Home Office* [2011] UKSC 35

33 Lord Kerr dissenting

*There cannot, after all, be an absolute rule that gisting must always be resorted to whatever the circumstances. There are no hard edges in this area of the law.*

1.40 Although the Government won in the case of *Tariq*, there remains considerable uncertainty as to the range of contexts in which gisting is and is not required. It could take many years of litigation for the courts to develop clear jurisprudence on this question that comprehensively accounts for all contexts. An alternative to this protracted period of uncertainty would be for the Government to clarify the position through legislation, using the existing court rulings as guidance. This question will be returned to in Chapter 2 of this Paper.

#### Disclosure of sensitive material into foreign jurisdictions

1.41 The *Binyam Mohamed* case (detailed in the box on page 9) started as a request for UK Government-held sensitive material to assist the claimant in military court proceedings in a foreign jurisdiction (in this case the USA). The judicial review of the Secretary of State's decision not to release the sensitive material drew on 'Norwich Pharmacal' arguments (see the box on the next page for more detail) for the first time in a detention case. As a result of this use of Norwich Pharmacal principles, the Government was for the first time at risk of having to disclose sensitive material to non-UK-security-cleared individuals for use in court proceedings outside the UK. The court in *Binyam Mohamed* acknowledged that PII applied to Norwich Pharmacal cases<sup>34</sup> but concluded that disclosure was justified in the interests of justice. The US Government at the time expressed its disappointment with this finding.

1.42 Relief under Norwich Pharmacal principles is intended to be exceptional and its application to a case such as *Binyam Mohamed* was, until the time of that case, unprecedented. It had not previously

been used where there was any question of disclosure causing a real risk of damage to the public interest in protecting national security. Nonetheless, it has been a growing area of litigation, with the Government having defended no fewer than seven such cases since 2008. The problem of the extension of the Norwich Pharmacal jurisdiction in this way has hitherto been confined to cases where disclosure of sensitive material is required to be made overseas, although the problem could in theory arise in the future in cases in which sensitive disclosure is ordered for use in proceedings within the UK.

1.43 Cases of this kind have also have a disproportionate impact on our international, diplomatic and intelligence relationships with foreign governments. Since *Binyam Mohamed*, the Government and its foreign government partners have less confidence than before that the courts will accept the view of Ministers on the harm to national security that would result from disclosure. Other cases – not all of which have resulted in public judgments – have raised similar questions in the case of UK-owned intelligence.

1.44 The Government is concerned that the UK's critically important and hard-earned secrets and those of our intelligence partners may be obtained by individuals through a recent development in our justice system. It is crucial that we rebuild the trust of our foreign partners in order to ensure that they can be satisfied that the range of sensitive material they share with us, and the communications on diplomatic channels, all of which take place with an understanding of confidentiality, will indeed remain confidential. We expect our intelligence partners to protect our sensitive material from open disclosure. We must do likewise if we are to sustain the international partnerships that are crucial to the Government's efforts to protect the public.



**Norwich Pharmacal: background**

A Norwich Pharmacal action is an equitable remedy developed by the courts in England and Wales, with an equivalent jurisdiction in Northern Ireland, requiring a respondent to disclose certain documents or information to the applicant. The respondent must either be involved or mixed up in wrongdoing by others, whether innocently or not, and is unlikely to be party to the potential proceedings. An order will only be granted where 'necessary' in the interests of justice. Orders are commonly used to identify the proper defendant to an action or to obtain information to plead a claim.

*Norwich Pharmacal Co & Others v Customs and Excise Commissioners*<sup>35</sup> was a case involving the owner and exclusive licensee of a patent for a chemical compound called furazolidone. Unlicensed consignments of the compound were imported into the UK, but Norwich Pharmacal was unable to identify the importers. The Commissioners held information that would identify the importers but would not disclose this, claiming that they had no authority to give such information.

The House of Lords held that where a third party who had been mixed up in wrongdoing had information relating to unlawful conduct, a court could compel them to assist the person suffering damage by giving them that information. This is now known as a 'Norwich Pharmacal Order'.

There is no equivalent remedy in Scotland.

1.45 The Government recognises that claimants in cases of this kind have often faced, or are facing, very difficult circumstances. Our objective is to ensure that individuals have proper access to the courts to address well-grounded claims and that, in doing so, critical national security partnerships are protected.

1.46 The consequences of striking the wrong balance in this area of law are potentially serious: we cannot afford for uncertainty in this area of the law to risk further the trust of our international intelligence partners, on whom we rely for our national security. The Government therefore wants to develop an improved framework for addressing these issues, one that fits coherently with other proposals in this Paper to manage sensitive information in cases heard in our own courts and builds sensibly on other relevant aspects of common law.

**Inquests involving sensitive material**

1.47 Over recent years there have been a small number of inquests in which sensitive material has been relevant to proceedings. In the majority of inquests in England and Wales<sup>36</sup> it has proved possible to deal with the challenges of handling sensitive information. Ad hoc solutions have been found that have enabled inquests to fulfil their purpose – determining how and in what circumstances the deceased person died, and providing a more thorough investigation where the circumstances of the death require it. For example, in the inquest into the 7 July 2005 bombings, the coroner ruled that she could not hold a closed procedure. This meant that she could not take account of some relevant material. PII applications were used to protect some of the sensitive material. In that case the coroner was able to reach a verdict and deliver a comprehensive 'Rule 43

35 [1974] AC 133

36 There is no coronial system in Scotland. Its equivalent is the Fatal Accident Inquiry system of judicial investigation of sudden or unexplained deaths, which is governed by the framework in the Fatal Accidents and Sudden Deaths Inquiry (Scotland) Act 1976. As a general rule, Fatal Accident Inquiries must be held in public (section 4(3)) and there is no Scottish equivalent of the provision in the England and Wales Coroners Rules allowing hearings in private. A recent review of the legislation recommended that the sheriff should be able to hold as a part of the inquiry as they think appropriate in private, but that has not (so date) been implemented. It is possible for a sheriff to compel the recovery or inspection of documents, and the attendance of witnesses, at a Fatal Accident Inquiry, though it is also possible to assert PII to exclude material from consideration by a Fatal Accident Inquiry.

When the relevant provisions of the Coroners and Justice Act 2009 are brought into force, the Fatal Accident Inquiry system will have jurisdiction in relation to service personnel and embedded civilian personnel even when those persons were killed abroad. Any Fatal Accident Inquiry in relation to these personnel could obviously raise issues of sensitive material.

Report' based on the evidence adduced in open court. She commented that the public summaries were detailed and, together with the disclosed documentation and the lengthy oral evidence, allowed the most intense public scrutiny of the relevant issues. However, because of the absence of any closed procedure, the Security Service was unable to put all the material before the Coroner, and while this did not prevent this inquest reaching its conclusion, the situation may be more challenging in future inquests.

1.48 It is conceivable that in a different case an inquest might not be able to properly investigate a death, for example if the coroner or jury were not able to take into account all relevant information. In some cases, coroners have concluded that the exclusion of material means that they have been unable to complete their investigation. Only when it has been possible to disclose more of that information (for example, with the passage of time) have such inquests been able to proceed.

1.49 In some cases where an inquest is not able to proceed, it may be possible to hold a public inquiry.<sup>37</sup> However, public inquiries are costly and complex (the four public inquiries established by the previous Government into deaths during the Troubles in Northern Ireland are expected to cost in excess of £300 million), and have always been an exceptional means of last resort to investigate deaths of significant public interest. The number of inquests where sensitive information is relevant continues to be small, but they are also likely to include particularly high-profile cases and will certainly also include cases where it would be absolutely disproportionate to have a public inquiry simply to be able to deal with a small amount of sensitive material.

1.50 This Paper will examine whether reform of inquests is warranted in order to enable more full and comprehensive conclusions, while ensuring that relevant sensitive material is safeguarded appropriately.

#### Article 2-compliant inquests

Article 2 of the ECHR requires a state to initiate an effective, independent investigation into any death occurring in circumstances in which it appears that agents of the state are, or may be, in some way implicated. This includes, for example, a death in state custody, or where a person has been killed by a state agent.

The nature and degree of the scrutiny required by Article 2 depends on the circumstances of the death, but broadly an investigation that is compliant with Article 2 of the ECHR is:

- initiated by the state
- independent of both the state and the parties
- effective and prompt
- open to public scrutiny and
- supports the participation of the next-of-kin so as to safeguard their legitimate interests.

Not all of the proceedings must necessarily be in public, and the degree of public scrutiny that is needed will vary from case to case. But the ECtHR has held that there must be:

*a sufficient element of public scrutiny in respect of the investigation or its results to secure accountability in practice as well as in theory, maintain public confidence in the authorities' adherence to the rule of law and prevent any appearance of collusion in or tolerance of unlawful acts.*<sup>38</sup>

In all cases the victim's next-of-kin must be involved to the extent necessary to safeguard their legitimate interests.<sup>39</sup>

37 Section 17A of the Coroners Act 1988 requires the adjournment of an inquest by the coroner if a public inquiry chaired by a judge is being or is to be, held into the events surrounding the death.

38 *Ramsahai v Netherlands*, App. No. 52391/99, judgment of 15 May 2007, para. 353; *Amin*, para. 60; *JL*, paras. 45 and 80

39 *Amin*, para. 20

### Summary and the case for change

1.51 These developments demonstrate that in recent years there has been a significant increase in the number, range and complexity of cases reaching the civil courts in which evidence of a genuinely sensitive nature is relevant to proceedings. Although still few in absolute terms relative to the overall number of non-sensitive cases being heard by our courts every year, these cases have a disproportionately high impact, including in terms of the strain that they place on our crucial relationships with international partners.

1.52 The well-established and understood mechanism of PII works well when the excluded material is only of marginal or peripheral relevance. It is much less successful as a mechanism for balancing the competing public interest in the administration of justice and the protection of national security in those exceptional cases where a large proportion of the sensitive material is of central relevance to the issues in the proceedings – judgments in these cases risk being reached based only on a partial and potentially misleading picture of the overall facts. When applied to proceedings such as *Carnduff*, which involve substantially all and only sensitive material, justice seems barely to be served as the case is struck out for a lack of a mechanism with which to hear it.

1.53 Where they are already provided for in legislation, CMPs do provide a satisfactory compromise in enabling both justice to be done and sensitive material to be safeguarded, and we are committed to looking for further opportunities to make the system as fair as possible. Areas for potential improvement and clarification do exist, primarily in terms of maximising the effectiveness of the role that can be played by Special Advocates, and in better clarifying the contexts in which courts will require summaries of sensitive material to be provided to the party affected by the CMP.

1.54 CMPs, however, are not available in many contexts in which, increasingly, they would benefit the interests of justice. It was their lack of availability in the Guantanamo civil damages claims, for example, that required the Government to reach an expensive out-of-court settlement, without the merits of the case having been argued. As the Secretary of State for Justice stated in Parliament,<sup>40</sup> at the time of the settlement:

*the alternative to any payments made was protracted and extremely expensive litigation in an uncertain legal environment in which the Government could not be certain that we would be able to defend Departments and the security and intelligence agencies without compromising national security.*

1.55 No other effective mechanism is available to the courts which might provide sufficient safeguards for sensitive material. Private hearings and confidentiality rings exist and operate effectively for less sensitive material, where the information can be shared safely between the parties and the problems caused by mishandling of information or leaking can be managed and contained. However, where national security is at stake, these mechanisms cannot give the required degree of assurance and there may be no way to manage or contain the harmful impact of making sensitive information public. This Government will never take risks with the security of our country.

1.56 The Government is well aware of the public debate and disquiet about the development of closed procedures. We reaffirm here our strong commitment to the general principle of open justice, but draw attention to the fact that, in certain, narrowly defined circumstances, the general principle can, and must, be set aside. As the Master of the Rolls stated in a recent speech,<sup>41</sup> this general principle can be set aside in narrowly defined circumstances because open justice is subject to a higher principle: that being, as Lord Haldane LC put it in *Scott v Scott*,<sup>42</sup> the:

40 Hansard, HC 16/11/10 col. 752

41 Lord Neuberger of Abbotsbury, *Open Justice Unbound*, Judicial Studies Board Annual Lecture, 16 March 2011. The same argument appears in 1.19 of the recent *Report of the Committee on Super-Injunctions*, under the chair of Lord Neuberger.

42 [1913] AC 417

*yet more fundamental principle that the chief object of courts of justice must be to secure that justice is done.*

1.57 In the next chapter of this Paper we examine a series of proposals aimed at improving fairness to all in civil proceedings in which sensitive information is relevant, and aimed at equipping the courts to better serve the interests of justice and of fairness. We believe it is possible to preserve procedural fairness while ensuring that cases can be heard, all relevant material considered and, where that material is sensitive, safeguarded appropriately. In an increasing number of proceedings, the Government must balance the desire to defend itself and receive independent judgments on its actions against the highly important duty to protect the public. These are unique pressures that normal parties in legal proceedings do not face. We must respond to the challenge of recent developments by finding improved ways for the courts and the Government to manage such cases. The Government believes it is in the public interest to strengthen the civil justice system in this area.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

## Chapter 2

# Sensitive material in civil proceedings: proposals and consultation questions

2.1 In this chapter we examine a series of proposals aimed at addressing the challenges that have been set out in the first sections of this Paper. The strength of support that we express for these proposals depends upon the extent to which they meet the Government's key principles for this Green Paper, as outlined in the Executive Summary. We have also looked at how practices have developed in other countries facing similar challenges and bound by similar legal commitments. While we have found no definitive solutions elsewhere, options that are used abroad are analysed where relevant and more detail about other countries' arrangements can be found at Appendix J.

**Consultation questions arise at the conclusion of each section and appear in boxes.**

### Enhancing procedural fairness

2.2 The first set of proposals in this Paper seek to **maximise** the amount of relevant material that is considered by the court while at the same time ensuring that, where the material is sensitive, it is protected from potentially harmful disclosure. We argue that it is **fairer** in terms of outcome to seek to **include** relevant material rather than to **exclude** it from consideration altogether and that the public interest is best served by enabling as many such cases as possible to be determined by the courts. (Proposals that deal with how material is protected when it is excluded from proceedings are discussed later in this Paper in the section entitled 'Safeguarding material' (page 33).)

### Proposal to expand CMPs to all civil judicial proceedings

2.3 CMPs have been a part of the framework of the courts of the UK since 1997. They are an existing mechanism that has been proven to work effectively and is familiar to practitioners. Making CMPs an option for the parts of any civil proceeding in which sensitive material is relevant would offer a number of benefits:

- ♦ In contrast to the existing PII system, CMPs allow the court to consider **all** the relevant material, regardless of security classification. A judgment based on the full facts is more likely to secure justice than a judgment based only on a proportion of relevant material.
- ♦ With both sides able to present their case fully to the court, it would be less likely that cases would have to be dropped or settled, as was the case in the Guantanamo civil damages claim, or struck out altogether, as in *Camduff*. CMPs would provide a mechanism for cases to be heard where at present the Government has no choice but to settle a claim against it, owing to its primary duty to safeguard national security.
- ♦ A broad extension would enable the courts to deal effectively with the challenges in all the contexts in which they arise.
- ♦ The contexts in which CMPs are already used have proved that they are capable of delivering procedural fairness. The effectiveness of the Special Advocate system is central to this, and it is examined in more detail later in this Paper (see paragraphs 2.24–2.38).
- ♦ CMPs reduce the risk of damaging disclosure of sensitive material.

2.4 CMPs should only be available in exceptional circumstances, and where used, every effort is and should continue to be made to have as much material considered in open court as possible. But in the small number of cases where sensitive material is crucial to the outcome, it is better that the court should be able to decide the case, despite the additional complexities a CMP might create, than – in a worst case – that the case should not be tried at all.

**The Government proposes to legislate to make CMPs available wherever necessary in civil proceedings.**

2.5 An appropriate mechanism for triggering the CMPs will help to ensure that they are only used where it is absolutely necessary to enable the case to proceed in the interests of justice. The principle of open justice is an extremely important one, and any departure from it should be no more than is strictly necessary to achieve a proper administration of justice.

2.6 There are a number of ways that a CMP could be triggered and it will be critical to get the balance right between the role of the Secretary of State (who is best placed to assess the harm that may be caused by disclosing sensitive information) and the judge (who must ensure that the interests of justice are served, including by ensuring that proceedings are as fair as possible, in the broadest sense).

2.7 Building upon existing models (see Appendix C), a proposed mechanism for triggering CMPs in new contexts is as follows:

- ♦ A decision by the Secretary of State that certain relevant sensitive material would cause damage to the public interest if openly disclosed, supported by reasoning and, where appropriate, by evidence.
- ♦ This decision would be reviewable by the trial judge on judicial review principles if the other side decides to challenge the Secretary of State's decision.
- ♦ If the Secretary of State's decision is upheld, a CMP is triggered. In the first phase of the CMP, the judge hears arguments from the Special Advocate and counsel for the Secretary of State about the appropriate treatment (in closed or

open court) of specific material or tranches of material, based on an assessment of harm to the public interest that would be caused by open disclosure – the aim here is to ensure that as much material as possible can be considered in open court. The ability of a Special Advocate to submit that any part of the closed material should become open material will continue until the conclusion of the proceedings.

2.8 The number of cases in which these procedures would be used will be a very small percentage of the overall number of civil cases passing through the courts each year – but these cases could be tried more effectively and with greater protection for sensitive material.

*Question: How can we best ensure that closed material procedures support and enhance fairness for all parties?*

2.9 Extending CMPs is not the only way that challenges around the handling of sensitive material in civil proceedings, including inquests, could be addressed. Other proposals are discussed later in this chapter, including:

- ♦ greater 'active case management' powers for judges (paragraphs 2.47–2.52)
- ♦ creation of a new 'specialist' court for national security cases (paragraphs 2.53–2.62)
- ♦ a wider remit for the Investigatory Powers Tribunal (paragraphs 2.63–2.71)
- ♦ putting PII on a statutory footing (paragraphs 2.74–2.82).

**CMPs and inquests**

2.10 Inquests are different to other forms of civil proceedings – they are a public, inquisitorial investigation into the cause and circumstances of violent or unnatural deaths, sudden deaths of unknown cause and deaths in custody. Some inquests require juries. Furthermore, if the death occurred in state custody or was caused by a state agent, then Article 2 of the ECHR will also require the involvement of the deceased's next of kin and a greater degree of public scrutiny. The number of inquests where sensitive information is relevant

continues to be very small, but they are also likely to include particularly high-profile cases. Because an inquest is a form of public inquiry, it can be difficult for it to proceed if sensitive material is relevant but cannot be disclosed in open court. PII has been effective in the vast majority of inquests in protecting sensitive material of marginal relevance, but in exceptional cases inquests are unable to proceed at all if highly relevant material is excluded because of its public interest sensitivity.

2.11 In a small number of high-profile recent inquests, sensitive material has been relevant but was protected by PII because it was too sensitive to disclose to the inquest. However, access to all the relevant information would enable the investigation to be more thorough and more effective. While there appear to be benefits in extending CMPs to all civil proceedings, the issues surrounding inquests are more complex and require separate consideration. If more information were to be put before an inquest, including sensitive material, this would of course have to be done in a way that can protect national security interests that might be damaged by unrestricted disclosure.

2.12 An inquest jury must be summoned by law when a death occurs in state custody or is caused by a state agent. This provides an additional independent element in public scrutiny of state action that is invaluable in ensuring public confidence in such investigations, particularly if it proved necessary to exclude the public from any part of an inquest. Proposals to exclude juries from inquests on national security grounds were brought forward by the last Government in the Counter-Terrorism Bill and the Coroners and Justice Bill, but were not enacted following clearly expressed views in Parliament about the measures. Those proposals are not revisited in this Green Paper.

2.13 Any risks posed by the disclosure of sensitive material to inquest juries could potentially be addressed by other, lesser measures. These could include:

- ◊ asking jurors to sign **confidentiality agreements**, though this would not of itself provide sufficient reassurance that sensitive information would be protected

- ◊ requiring jurors to undergo **security clearance** to the same level as Special Advocates, thus enabling them to hear the sensitive material under consideration. This would provide the greatest level of protection to sensitive material, but this type of vetting is an intrusive process, requiring detailed background checks; it would also be costly and time-consuming. While this type of vetting works well in the employment context (for example, where someone chooses to submit to it as a condition of taking a particular job), requiring it of a person fulfilling their civic obligations by sitting as a juror is a different matter

- ◊ **light-touch vetting** of juries (for which there is precedent in criminal cases in England, Wales and Northern Ireland; here, additional checks over and above criminal record checks to identify disqualified jurors can be made in certain circumstances with the permission of the Attorney General, though these arrangements are rarely used). This model could be applied to inquest juries as well. While the level of checks permitted provides a lesser degree of protection for sensitive material, in some cases – depending on the circumstances – it may be worth considering.

2.14 Inquests play an important role for families in understanding and coming to terms with the death of a loved one. This is recognised by the status given to the deceased's relatives in a coroner's inquest; as 'properly interested persons' (PIPs) they are entitled to examine witnesses. This is also recognised by the ECHR, which requires that where Article 2 is engaged, an investigation into a death must provide for involvement of the deceased's next of kin to the extent that protects their interest. Families can also provide vital information to assist the coroner in investigating a death.

2.15 Improving the way that sensitive information is handled in inquests could help families to better understand the circumstances of the death of a relative, but protections would need to be put in place to safeguard national security interests. Options to do this could include:

- ◊ **security vetting of family members** in order to enable them to see and hear sensitive material but, as with jurors, this would be an

intrusive process and it could be extremely distressing for a family grieving the loss of a relative. Additionally, some means would have to be provided to exclude family members in the event that they did not wish to be vetted or were not cleared to see the material

- ✦ amending or adding to the Coroners Rules to allow the coroner to have a CMP for part or all of an inquest, and provide for families to receive 'gists' of sensitive material and be represented by Special Advocates when sensitive evidence is presented to the inquest.

2.16 Families are not the only people who can be PIPs in an inquest. The definition of a PIP is set out in Rule 22 of the Coroners Rules 1984. As well as family members, PIPs can include anyone alleged to have caused or contributed to the death, or anyone that the coroner thinks should be granted PIP status. If steps were taken to introduce CMPs into inquests, then provision should be made in certain circumstances for Special Advocates to represent the interests of any other PIPs excluded from any closed part of the inquest, thereby enabling them to question witnesses.

2.17 Normally, most inquests are conducted by a coroner, who is either a lawyer or a doctor appointed to investigate deaths. In certain circumstances, a judge can be appointed as a coroner and conduct an inquest (as happened in the 7 July 2005 inquests, which were conducted by Lady Justice Hallett). Judges are likely to have greater experience at dealing with complex cases involving sensitive information, and some types of sensitive information (such as material derived from the interception of communications) can be disclosed to a judge in certain circumstances, but not to a coroner. Where an inquest is dealing with sensitive information there could therefore be benefit in a judge being appointed as coroner to hear the case.

2.18 The alternative to these options would be to continue to rely on PII in cases in which sensitive material is relevant to proceedings. Public inquiries, as alternatives to inquests, might also in exceptional circumstances have to be established, as is currently provided for in the Inquiries Act 2005. However, public inquiries can take a long time to complete and are often very expensive.

2.19 These issues are finely balanced and public views are sought on these particular challenges.

**Question: What is the best way to ensure that investigations into a death can take account of all relevant information, even where that information is sensitive, while supporting the involvement of jurors, family members and other persons?**

#### *Fatal Accident Inquiries in Scotland*

2.20 Given the entirely different system in Scotland, the UK Government is engaged with the Scottish Government and Crown Office to determine how best to effect changes in Scotland.

#### *Northern Ireland inquests*

2.21 The Government recognises that specific circumstances apply to inquests in Northern Ireland. The coronial system is devolved and inquests in Northern Ireland operate under a different statutory framework. Particular to Northern Ireland, there are also 34 outstanding 'legacy inquests' into deaths that occurred during the Troubles.

2.22 The Government would welcome the views of political parties, families, non-governmental organisations and legal organisations on whether any aspects of these proposals should apply to inquests in Northern Ireland. We will also be consulting with the Northern Ireland Justice Minister, the devolved administration and those who operate the system in Northern Ireland.

2.23 The 'legacy inquests' into deaths that occurred during the Troubles raise specific issues. The Government is extremely mindful of the important role that families have played in these proceedings to date. As the Consultative Group on the Past said in its 2009 report:

*the outstanding inquests raise important questions and... some families have fought for many years through the courts to establish their rights in these proceedings.*

However, the Government does recognise the limitations of the current arrangements from the perspective of bereaved families. The Government



recognises that new arrangements on disclosure may help to increase the confidence of the families involved that all relevant information could be considered by an independent figure rather than being excluded from the process entirely under PII.

*Question: Should any of the proposals for handling of sensitive inquests be applied to inquests in Northern Ireland?*

#### Improvements to the Special Advocate system

2.24 How well the Special Advocate system works will be a critical factor in the success of the proposed expansion of CMPs into new contexts. Special Advocates are effective in representing the interests of individuals excluded from the whole or parts of proceedings, but there may be ways that the existing arrangements can be further improved, in particular:

- ◊ additional training on intelligence analysis and assessment methods in order to enable more rigorous challenge of closed material
- ◊ better arrangements for communication with the party whose interests they are representing after service of closed material.

2.25 Special Advocates attend a one-day training course facilitated by the Security Service which explains intelligence processes, including how intelligence is assessed (including its reliability), how investigations are prioritised, what sort of actions are taken and when and why. The training includes the examination of case studies from the perspective of intelligence analysts. This training is intended to better equip the Special Advocate to represent the interests of an excluded person during the CMP by better enabling them to challenge sensitive material during closed hearings.

2.26 Feedback from Special Advocates on their training has been overwhelmingly positive but it is clear that, while the training meets all requirements for newly appointed Special Advocates, there is currently a gap in training provision for experienced Special Advocates who either require refresher modules, re-attendance

at the introductory course or specific training on particular issues that commonly arise in CMPs.

**The Government will make available increased training for Special Advocates where required.**

This will be particularly important if CMPs and Special Advocates are available in a wider range of types of proceedings.

2.27 If CMPs are used more widely then there will be a greater range of civil proceedings in which Special Advocates may have to operate in the future. These types of contexts may raise more complex issues to be dealt with in the litigation. Consequently, in addition to further training sessions that Special Advocates may feel that they require, **they will be provided with sufficient resources in terms of independent junior legal support to ensure that they are able to carry out their function as effectively and thoroughly as possible.**

2.28 Concerns have been expressed around whether the restrictions on the ability of Special Advocates to communicate with the excluded individual after seeing the closed material without permission of the court (on notice to the Secretary of State) affects Special Advocates' ability to discharge their function of representing the individual's interests in the CMPs.

2.29 A Special Advocate may take instructions from the individual before they have seen the closed material. There is currently no absolute prohibition on communication between the Special Advocate and the individual after service of the closed material. Such communication can occur, providing it is with the permission of the court. The court must notify the Secretary of State when the Special Advocate seeks permission, giving the Secretary of State time to object to the communication if it is considered necessary in the public interest, although the final decision is that of the court. However, in practice, Special Advocates have only rarely sought permission from the court to communicate with the individuals whose interests they are representing after service of the closed material, owing at least in part to concerns that such communication, once requested of the Secretary of State, would reveal litigation and other tactics and strategy and consequently unfairly benefit the Government side.

2.30 The proposed communication may pertain to questions that the Special Advocate would wish to ask the individual **about**, or even remotely **linked to**, the closed material. A Special Advocate may believe that they are able to construct communication in such a way that would not risk damage to the public interest, but the answer to which would, nonetheless, aid the Special Advocate's ability to represent the interests of the individual. However, without detailed knowledge of the investigation, or other linked investigations, the Special Advocate could inadvertently disclose sensitive information, for example the identity of an agent or details of related ongoing investigations. In order to know whether the proposed communication could be damaging to national security, those familiar with the day-to-day operation of that (and connected) investigation(s) must be able to review any proposed communication.

2.31 Any such communication would have to be cleared through the Secretary of State on advice from the relevant experts, most commonly officials in the Agencies familiar with the case in question and with an understanding of the potential for public interest damage to be caused.

2.32 Reforms in this area could enhance the ability of Special Advocates to discharge their duties. The Government is accordingly giving consideration to all feasible options.

2.33 A properly functioning 'Chinese wall' may be an innovation that could enhance the willingness of Special Advocates to make use of existing procedures in communicating with the excluded individual(s) after the service of closed material. One possible solution could be in the placing of a Chinese wall mechanism between government counsel (including Treasury Solicitors) and those clearing the communications request within an Agency. Treasury Solicitors and counsel would not be able to view the proposed communication. This arrangement could be further strengthened by a protocol which would confirm that within the Agencies, the minimum number of people necessary to carry out the security check would be involved. The Government is accordingly giving consideration to such a mechanism and protocol, as well as considering the resource and

deliverability implications for other Chinese wall models which place the 'wall' in different positions within the Government side.

2.34 One difficulty will be to regularly source an official, or cadres of officials, from within the relevant government department or Agency who will have sufficient knowledge of the case, the sourcing of the relevant material, issues around the litigation itself and the context of the case relative to other similar cases, who will as a result be able to provide definitive assessments of the risk level of proposed Special Advocate communication, but who is not in contact with, nor can have contact with, the litigation team itself and government counsel.

2.35 Special Advocates may argue that, in some instances, their proposed communication will relate only to purely procedural or administrative matters that relate solely to directions in the case, as opposed to substantive factual or legal issues and that therefore there is no requirement for the Government to clear these communications. However, the Special Advocate is not in a position to fully determine harm to the public interest and thus it does not seem possible to create 'categories' of communication which would require different clearance procedures. **Further analysis of whether 'categorisation' of communication is possible continues to be undertaken.**

*Question: What is the best mechanism for facilitating Special Advocate communication with the individual concerned following service of closed material without jeopardising national security?*

2.36 Special Advocate communication requests have to be cleared not only by the Secretary of State but also the judge. Some Special Advocates have voiced concern that here too they are potentially exposing their strategy and the strengths or weaknesses of their case to the judge. One solution would be for a separate judge to deal with applications to communicate with an excluded person. The Government has no concerns regarding this proposal from a national security perspective. However, there are clear resource and administrative implications of involving an

additional judge in the administrative aspects of a case involving CMPs, including a potential delay to proceedings. Given that this is likely to be a less significant issue than exposing litigation strategy to the other side, and that it seems unlikely that a judge would need to excuse themselves from a case as a result of something heard during the course of an application made during a case, **we consequently do not propose involving a separate judge.**

2.37 The Special Advocate system is provided for in legislation in 14 different contexts of civil proceeding as well as performing a slightly different role in criminal trials in exceptional circumstances. In each context, the system operates along the same broad lines (unless affected by specific case law, such as *AF (No.3)*<sup>1</sup>), based on the original model used in SIAC.

2.38 The one exception to this uniformity of system across contexts is in employment tribunal hearings – the provisions governing communications after service of closed material in employment tribunal hearings are not as clearly defined as in the other contexts in which Special Advocates are provided for in statute.<sup>2</sup> The Government sees no reason why, in principle, the Employment Tribunal Rules on Special Advocates should not be brought into line with other Special Advocate regimes and **we propose making the necessary amendments to the Employment Tribunal Rules<sup>3</sup> in order to harmonise the Special Advocate system across contexts.** This will enable Special Advocates to operate more readily in different courts and tribunals and bring a greater degree of consistency to proceedings in which

Special Advocates are appointed. Consideration of other concerns raised about the operation of the Special Advocate system can be found at Appendix E.

**Clarifying the requirements for disclosure of damaging summaries of sensitive material: the 'AF (No.3)' principle of 'gisting'**

2.39 In this section we examine the risks and benefits of seeking, through legislation, to clarify the range of contexts in which it is and is not necessary to provide an individual with sufficient information about the allegations against them, however sensitive, to allow them to give effective instructions to their Special Advocate, as set out in the June 2009 Law Lords judgment in *AF (No.3)*<sup>4</sup> (see Appendix D). At present no such clarity exists, other than in relation to the now repealed powers set out in Part 4 of the Anti-terrorism, Crime and Security Act 2001; and in stringent control orders and financial restriction orders where such a disclosure requirement has been imposed by the courts.

2.40 However, the Supreme Court recently ruled in *Tariq*<sup>5</sup> that 'gisting' is not required in employment tribunal proceedings concerning security vetting. Furthermore, it is clear from the Strasbourg Court's decision in *Kennedy*<sup>6</sup> that 'gisting' is not necessary in cases concerning secret surveillance. In addition, there are categories of proceedings to which Article 6 of the ECHR does not apply because they do not determine 'civil rights': in particular, immigration cases – including SIAC cases – fall outside Article 6.<sup>7</sup>

1 *Secretary of State for the Home Department v AF (No.3)* [2009] UKHL 28

2 See rule 54(2)(b) of Schedule 1 to the Employment Tribunals (Composition and Rules of Procedure) Regulations 2004 (S.I.2004/1861). Compare rule 36 of the Special Immigration Appeal Commission (Procedure) Rules 2003 (S.I. 2003/1034).

3 Procedures set out in Schedule 2 to Employment Tribunals (Constitution and Rules of Procedure) Regulations 2004 S.I. 2004/1861.

4 *Secretary of State for the Home Department v AF (No.3)* [2009] UKHL 28.

5 *King v Ministry of Defence* [2011] UKSC 35

6 *Kennedy v UK* (2011) 52 EHRR 4

7 *Maaouia v France* (2001) 33 EHRR 42; *W (Algeria) v Secretary of State for the Home Department* [2010] EWCA Civ 898, at [32]. However, Article 5 (4) and consequently the disclosure requirement does apply to bail proceedings before SIAC: *B. (Iran) v Upper Tribunal* [2009] EWHC 3052 (Admin).

2.41 However, it is unclear how far Article 6 may require 'gisting' in other categories of cases. In his judgment in *Tariq*, Lord Dyson stated<sup>8</sup> that:

*In many cases, an individual's case can be effectively prosecuted without his knowing the sensitive information which public interest considerations make it impossible to disclose to him.*

2.42 The Supreme Court did not seek to define the 'many cases' to which Lord Dyson referred in his judgment.<sup>9</sup>

2.43 It would be possible for Parliament to seek to legislate to clarify the contexts and types of civil cases in which the 'AF (No.3)' disclosure requirement does not apply.

2.44 Clarity on these disclosure requirements would create a greater degree of predictability in CMP litigation, where in many contexts uncertainty over requirements is spawning considerable satellite litigation away from the substantive proceedings. For the Government, knowing in advance of proceedings that there will or will not be such a requirement means that the Government may embark on non-prosecution actions against (for example) suspected terrorists, or defend cases that crucially depend on sensitive material, without the risks that the case might have to be abandoned or conceded midway through, due to undeliverable and unforeseen disclosure requirements set out by the court.

2.45 It would of course still be possible for affected individuals to bring proceedings under the Human Rights Act 1998 (HRA) arguing that the legislation preventing them from receiving the 'gist' was incompatible with the ECHR. But in such proceedings, the court would have the benefit of Parliament's clearly expressed view about how the balance between the competing interests should be struck.

2.46 For the individual who does not need to be provided with a 'gist', owing to the strong countervailing public interest in protecting national

security, the courts will ensure that their case is tried with sufficient procedural fairness and that they may benefit from the other safeguards such as a Special Advocate who will, on the individual's behalf, work to ensure that as much of the case as possible is heard in open court.

**Question: If feasible, the Government sees a benefit in introducing legislation to clarify the contexts in which the 'AF (No.3)' 'gisting' requirement does not apply. In what types of legal cases should there be a presumption that the disclosure requirement set out in AF (No.3) does not apply?**

#### More active case-management powers for judges

2.47 In this section we look at whether it is possible to replicate any 'best practice' methodology from the more 'inquisitorial' style of proceedings that is used in some other ECHR-compliant European jurisdictions. The intention in looking at European best practice is to see whether elements of models in other jurisdictions could play a role in **conjunction with** our central proposal for more widely available CMPs, in order to deliver as great a degree of procedural fairness as possible, while at the same time realising the other objectives of this Green Paper.

2.48 Inquisitorial proceedings are proceedings that are controlled and directed by the judge rather than the parties. Other countries have systems which involve more inquisitorial elements than the UK's system. It is sometimes said that the objective of an 'adversarial' system is to settle the dispute as defined by the parties, whereas the objective of an 'inquisitorial' system is to ensure that an objectively just outcome is achieved. The legal system in the UK is rooted in the adversarial system. There are very few legal contexts or processes in the UK that operate primarily through an inquisitorial system – coroners' inquests, as mentioned earlier, are one

8 At [147] of *King v. Hone & Ors* [2011] UKSC 35

9 But the court pointed out that the *A v UK* and *AF* decisions concerned the special cases where the liberty of the individual was at stake.

such rare exception. Given the overwhelmingly adversarial tradition in the UK justice system, the introduction of greater elements of an inquisitorial system into our courts would be a significant culture shock and methodological upheaval for the judiciary.

2.49 It would not be possible to introduce entirely inquisitorial proceedings into UK courts. The right to a fair hearing in Article 6 of the ECHR implies the right to adversarial proceedings, according to which the parties must normally have the opportunity to see and comment on the evidence against them.<sup>10</sup>

2.50 However, it might be possible to introduce a greater inquisitorial element at some stages of the proceedings. For instance, having an inquisitorial phase precede adversarial proceedings might result in the judge deciding on a narrower scope for the case. This could significantly streamline proceedings and related disclosure exercises as the judge would have already decided which evidence was relevant. However, once the adversarial element of the proceedings commences, the effect of having run the inquisitorial phase at the outset will not in itself provide the required safeguarding of sensitive material without PII or CMPs. This is a further reason why the analysis in this section must be considered in conjunction with the proposal in paragraph 2.4 above.

2.51 Granting the judge more powers through the inquisitorial model is unlikely to result in a more efficient process. While the role of the Special Advocate might diminish slightly as the judge takes on a greater role in testing, challenging and probing material, the judge will require greater staffing and resourcing in order to carry out the inquisitorial pre-hearing phase.

2.52 The Government has concluded that there appear to be no clear benefits to introducing an inquisitorial system into our courts purely for the management of civil proceedings involving sensitive material. It would not in itself increase the number of cases that can be dealt with effectively in the justice system as it would be reliant on a

CMP (and adversarial) phase to proceedings. Its introduction could represent a significant cultural and procedural upheaval in the British judicial system which would be difficult to justify for the small number of exceptional cases that it would be seeking to address. **The Government does not propose to introduce inquisitorial elements or more active case-management responsibilities for judges in cases involving sensitive material.**

### Specialist court structures

2.53 This section looks at whether civil legal proceedings that require an examination of sensitive material should be heard in a specialist court, with appropriate safeguards that serve both the interests of justice and of national security.

2.54 There exist already in the judicial system many specialist courts and tribunals. These are not independent bodies, but administrative divisions and subdivisions of the courts and tribunals. Thus, for example, the Queen's Bench Division of the High Court has within it the Administrative Court, the Admiralty Court, the Commercial Court and the Mercantile Court, to cite but a few.

2.55 Although structured along slightly different lines, specialist chambers of tribunals also exist, as do separate tribunals such as the Investigatory Powers Tribunal (IPT), SIAC and Employment Tribunals, which are also examples of specialist court/tribunal structures within our existing system.

2.56 Previous governments have not previously sought to establish a 'national security' court or tribunal for the hearing of cases in which most or all of the content may be sensitive. Rather, national security is an aspect of disputes which may arise in any field of law. Thus employment or immigration cases will be heard by the specialist tribunals that deal with those types of case even if they have national security sensitive elements. National security interests arise as individual rights are determined and issues between parties are set out.

<sup>10</sup> E.g. *Martinie v France*, App.No.58675/00, (2007) 45 EHRR 15, at [45]-[50]; *Hudakova v Slovakia*, App.No.23083/05, judgment of 27 April 2010, at [25]-[32].

2.57 Our research on international practice in this area confirmed that none of the countries we surveyed had established a specialist court solely for the purpose of hearing national security cases, and we did not find examples of specific government efforts to promote judicial specialisation.

2.58 In the Supreme Court judgments of *Al Rawi*<sup>11</sup> and *Taniguchi*,<sup>12</sup> Lord Brown reflected on whether the IPT, or a body which is similar, could provide a solution to the difficult issues raised in cases against the intelligence services or involving security vetting decisions. The Government has given such issues careful consideration, and we examine the role and remit of the IPT in paragraphs 2.63–2.71.

2.59 It would be possible to create a new specialist court or tribunal, with its own rules and nominated judges, that exclusively considers national security cases. This would require primary legislation. Such a court would be very different from the existing specialist courts and tribunals, which are made up of judges who have specialist knowledge of a particular technical area of law (such as employment, tax or immigration). The advantage of a specialist court or tribunal of that sort is that it can deal efficiently with the large number of cases falling within that area, because the judges are already familiar with the technicalities and do not need to have the fundamental concepts explained to them each time. In contrast, a specialist court would deal with a wide range of substantive law; the only aspect that the cases would have in common is that they would all involve sensitive evidence.

2.60 Overall, we consider that proposals to establish a specialist court carry significant risks and unclear benefits. Establishing such a structure would represent a significant cultural upheaval for many members of the judiciary and would unnecessarily distinguish cases involving sensitive material from other types of proceedings, against the usual case management practices of our courts.

2.61 We propose that, rather than establishing or designating a particular court for hearing national security cases, the specialised procedures of a CMP should be available in the ordinary courts when the exceptional circumstances of a particular case require them. The judge who sits in the open court would also hear the closed sessions, so the effect of moving into a CMP would simply be to remove all persons from the court with the exception of the judge, government counsel and the Special Advocate.

2.62 The risk of having CMPs available in the ordinary courts is that the judge might have little or no experience of closed hearings and might additionally lack experience of handling sensitive material and recalling what can and cannot be discussed as the court moves between open and closed hearings. In practice, this risk is minimal given that cases tend to be allocated to judges with experience of dealing with the subject matter or the issues in the case. It is usually possible to determine in advance of a case starting whether sensitive material might be relied on by one or other party and this can therefore be taken account of in the allocation process by the judges themselves.

*Question: At this stage, the Government does not see benefit in introducing a new system of greater active case management or a specialist court. However, are there benefits of a specialist court or active case management that we have not identified?*

#### The Investigatory Powers Tribunal

2.63 The IPT was created<sup>13</sup> to provide a judicial body to hear and determine complaints and HRA- and ECHR-based claims against the Agencies, including in respect of conduct by them. The IPT is an important component of the control

11 *Al Rawi v Security Service* [2011] UKSC 34, at [86]

12 *Taniguchi v Foreign and Commonwealth Office* [2011] UKSC 35, at [94]

13 By S.65 of the Regulation of Investigatory Powers Act 2000.

mechanism established by RIPA to ensure that the exercise of investigatory powers by the Agencies and other public authorities, and any other conduct by the Agencies, is subject to adequate and effective safeguards against abuse.

2.64 In this section, we consider whether the remit of the IPT could be expanded to hear more civil proceedings that centrally involve national security sensitive material, developing the comment of Lord Brown in his judgment in *Al Rawi*.<sup>14</sup>

2.65 Currently the IPT has two primary functions in this area.<sup>15</sup> First, it has exclusive jurisdiction to hear and adjudicate on ECHR-based claims against the Agencies. Second, to consider and determine complaints by individuals against the Agencies. These functions mean that the IPT has a significant role in providing scrutiny and oversight of conduct by, and the ECHR-compliance of, the Agencies.

2.66 The IPT's rules ensure that it can consider and determine complaints and adjudicate on ECHR-based proceedings without breaching the 'neither confirm nor deny' principle or revealing information about techniques and capabilities that would prejudice national security or be contrary to the public interest.

2.67 Given the IPT's existing statutory framework for securely handling sensitive material, the Government has considered the merits of expanding the remit of the IPT in order that it may hear more (or all) non-criminal cases involving national security sensitive material.

2.68 There is already statutory provision to expand the remit of the IPT to some extent through the commencement of sections of RIPA that are not in force. This would:

- ♦ enable the IPT to consider and determine references to it by an individual who has suffered detriment in civil proceedings as a result of the application of section 17 of RIPA (which restricts the use of warranted intercept in legal proceedings)<sup>16</sup>
- ♦ enable the IPT to consider such other proceedings against the Agencies as are allocated to the IPT in accordance with an order and approved by Parliament and then made by the Secretary of State.<sup>17</sup>

2.69 If the IPT's remit is expanded then the mechanisms and rules of the IPT may have to be amended in order to ensure continued compliance with requirements under Article 6 of the ECHR, in the new contexts in which the IPT would operate.<sup>18</sup> Special Advocates may have to be appointed to represent the interests of the individual in cases falling within the IPT's amended jurisdiction. An appeals procedure would have to be provided against any exercise by the IPT of its new jurisdiction.<sup>19</sup>

2.70 Given these necessary large-scale and resource-intensive amendments to the current working practices of the IPT, there are no clear benefits to expanding the remit of the IPT through RIPA relative to the primary recommendation of this Green Paper, namely to make CMPs more available in statute, for use in civil proceedings in exceptional circumstances. The secure handling of sensitive material, together with the sufficient procedural fairness that CMPs have been shown to deliver in SIAC and other contexts, lead the Government to express in this Paper a strong preference for their expanded availability, rather than a significant reconfiguration of the IPT.

14 *Al Rawi v Security Service* [2011] UKSC 34, at [86]

15 In addition, a role for the IPT is also provided for in paragraph 14(3)(b) of Schedule 2 to the Equality Act 2006 and S.69B(2)(b) of the Northern Ireland Act 1998, as inserted by the Justice and Security (Northern Ireland) Act 2007.

16 S.65(2)(c) of RIPA

17 S.65(2)(d) of RIPA

18 In *Kennedy v UK* (2011) 53 EHRR 4, the ECtHR confirmed that the IPT's procedures within its present remit comply with Article 6.

19 S.67(9) of RIPA, not presently in force.

2.71 The IPT is a specialist tribunal that provides a forum for the proper and effective judicial determination of a specific type of claim. The IPT rules provide specific protections for sensitive intelligence material while ensuring that the IPT can take into account all evidence, irrespective of whether it would be admissible in the ordinary courts. This involves a departure from the usual procedures of adversarial courts and, as such, these procedures should be used sparingly. The resource-intensive IPT model would not be appropriate for civil damages claims, which typically may involve a large number of government departments.

**Question: The Government does not see benefit in making any change to the remit of the Investigatory Powers Tribunal. Are there any possible changes to its operation, either discussed here or not, that should be considered?**



### Safeguarding material

2.72 The previous section, 'Enhancing procedural fairness', focused on maximising the amount of material disclosed in court proceedings through proposals to permit the safeguarded disclosure of relevant sensitive material through a wider availability of CMPs.

2.73 An alternative approach would be to strengthen the mechanisms through which sensitive material could be excluded from the court process, thereby avoiding damaging disclosure. We discuss this approach here. None of the proposals considered here meet our objective of allowing the court to consider as much relevant material as possible. However, if carefully applied, they could provide an important alternative or complement to the proposals in the previous section, in support of the objectives of protecting material in a manner consistent with domestic law and ECHR, reducing the number of cases that have to be dropped, settled or struck out, and achieving this by building on existing processes.

### Enshrining PII in legislation

2.74 While CMPs, if adopted, would significantly reduce the number of cases in which a PII claim was necessary, there is still a need to consider PII and other existing procedures, refining and adapting them as a complement to CMPs. The overarching question for consultation in this area is as follows:

**Question: In civil cases where sensitive material is relevant and where closed material procedures not available, what is the best mechanism for ensuring that such cases can be tried fairly without undermining the crucial responsibility of the state to protect the public?**

2.75 The current system of PII is well understood and generally operates effectively, particularly in cases where the PII claim is confined to sensitive material which is of only marginal or peripheral relevance. The onus rests on the executive to exercise rigour, candour and responsibility in making PII claims. Damage caused by poorly justified assertions of damage to public interest cannot be overestimated; Ministers (and their officials) must ensure that claims are well reasoned, necessary, proportionate and supported by evidence. Ministers have a duty to claim PII where they assess that disclosure would cause real harm to the public interest and the balance of public interests is in favour of non-disclosure.

2.76 In a small number of cases, courts have taken a decision to order disclosure of material, despite a claim by the Government that the material should be subject to PII. One of the most well known of these was *Binyam Mohamed*.<sup>20</sup> In that case and for specific reasons, while acknowledging that the Foreign Secretary's views should be given great weight, the Court of Appeal did not uphold the Foreign Secretary's claim to PII for material passed through intelligence channels to the UK.

2.77 Examples of cases in which the courts do not uphold the Government's claim to PII are few and the courts have stated<sup>21</sup> that they will continue to give weight to Ministerial views on the damage to national security that would result from disclosure. However, the fact of these cases, together with others where there has been a very real risk of a certificate not being upheld, mean that the Government and its partners have less certainty that they will be able to continue to protect material in court.

2.78 It would be possible for Parliament to provide the courts with clearer guidance in statute on the application of PII in more difficult areas,

20 *R (Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 65. The court would have upheld the PII certificate if there had not been evidence that the relevant information had already been put into the public domain in Judge Kessler's Memorandum Opinion in the US District Court for the District of Columbia: see [191], [203] and [295].

21 Court of Appeal judgment in *Binyam Mohamed* [2010] EWCA Civ 65: 'It would require expert evidence for a judge to differ from an assessment of this nature made by the Foreign Secretary. National security... is absolutely central to the fundamental roles of the Government... In practical terms, the Foreign Secretary [is] far better informed, as well as having far more relevant experience, than any judge, for the purpose of assessing the likely attitude and actions of foreign intelligence services.'

clearly defining the parameters of the balancing test when determining public interest imperatives around disclosure of sensitive material. In order for the statutory test to provide more stability and certainty than provided by the existing convention of judicial 'deference' to the Executive on national security arguments, the test would have to include statutory presumptions against open disclosure of sensitive material.

2.79 One such presumption would be against disclosure of sensitive material owned by foreign governments, obtained via intelligence relationships working on the basis of the Control Principle. The principle is central to all liaison relationships, so reciprocal adherence is as much about protecting the UK as it is anyone else's material. However, before considering legislation including statutory presumptions, the Government would need to analyse the full range of issues that such an approach might raise. For example, a procedure which sought to exempt **classes** of documents, rather than specific documents based on sensitive content, would be potentially controversial as it would return to class PII claims, which UK law has moved away from since the 1990s.<sup>22</sup>

2.80 It may therefore be most appropriate for any presumption to be rebuttable – that the courts would retain the power to decide in favour of disclosure. If this approach were followed, the court-led PII balancing exercise would thus remain at the heart of the process, and provide little advance on the current system in terms

of providing stability and certainty for the UK Government and our partners. A marginal benefit is that the courts would be bound to apply the statutory test and take account of the clearly expressed will of Parliament.

2.81 Finally, there is a risk that statutory presumptions of any kind, in creating a presumption of protection of certain types of material over others, could have the effect of diminishing the protection afforded to other types of material, for example the very large volume of domestically generated intelligence and other sensitive material. This could be avoided by defining very widely the types of material protected, but this would arguably reduce their impact on court decision-making.

2.82 As an established common law principle, PII will retain a residual role in civil proceedings even if broader reforms are introduced. However, if the proposals recommended in this Green Paper are pursued, we would envisage a much reduced role for PII. Furthermore, given the difficulties around the use of statutory presumptions, we judge that it would be difficult to ensure that legislation on PII could offer a substantial advance on existing expectations of judicial deference to executive advice on national security. In light of this, we judge that pursuing legislation on PII would deliver marginal benefits, and that there are better ways, explored elsewhere in this Paper, to strengthen our ability to protect material. **The Government does not propose to legislate for PII.**

<sup>22</sup> The Scott Report considered PII, in the context of the criminal Matrix Churchill trial, and concluded that legislation on PII was neither necessary nor desirable. The Government agreed with this recommendation. The report was also critical of the Government's use of 'class claims'.

### Addressing the challenge of court-ordered disclosure of sensitive material into foreign legal proceedings

2.83 In this section, we examine several options for resolving the difficult issues which arise in cases where a claimant seeks disclosure of sensitive material held by the Government in order to assist in another set of proceedings, usually taking place abroad.

2.84 The Government's aim in this area is to develop an improved legal framework that fits coherently with the procedures for managing sensitive information in cases heard in our own courts and with the established common law principles of PII and, above all, that avoids the development of new routes of disclosure that could fundamentally undermine the UK's national security co-operation with key partners.

2.85 The Norwich Pharmacal jurisdiction enables a claimant to obtain disclosure of information from a defendant who is mixed up, whether innocently or not, in arguable wrongdoing of a third party. In summary, there are five elements to the test that a claimant must satisfy in order to succeed in their claim, namely:

- ◊ there must be arguable wrongdoing on the part of a third party
- ◊ the defendant must be mixed up in that arguable wrongdoing, however innocently
- ◊ it must be necessary for the claimant to receive the information by making the Norwich Pharmacal application; put another way, if the information can be obtained by another route, the court may not grant the order
- ◊ the information sought must be within the scope of the available relief; it should not be used for wide-ranging disclosure or evidence-gathering and it is to be strictly confined to necessary information
- ◊ finally, the court must be satisfied that it should exercise discretion to make the order sought.

2.86 Norwich Pharmacal applications are a special category of civil claims. In many claims which engage national security interests, the purpose of the application has been to obtain disclosure of material in order to assist the claimant in other proceedings. That is in contrast to other types of civil claim which have been discussed in this Paper, where disclosure of material is just one aspect of the proceedings but is not the whole purpose of bringing the claim.

2.87 Accordingly, for these difficult Norwich Pharmacal applications against the Government, while the Government is likely to need a CMP where the detail of the sensitive material is being discussed, implementing that CMP is not going to be sufficient to protect the sensitive material because disclosure of that material is exactly what is being sought. Hence in addition to consulting on implementing CMPs in civil damages claims, it is necessary for the Government to consider and consult upon the future of Norwich Pharmacal proceedings against the Government where sensitive material is involved.

2.88 The Government starts from the perspective that, in recent years, access by members of the public to information held by public authorities has been greatly enhanced, principally through the Freedom of Information Act 2000 and the Data Protection Act 1998. The Government is committed to openness and transparency, but it is to be noted that both Acts incorporate exemptions for national security material<sup>23</sup> which are not present in the Norwich Pharmacal jurisdiction.

2.89 The Government has examined a range of options for reducing the potentially harmful impact of court-ordered disclosure of sensitive material in Norwich Pharmacal claims.

2.90 We considered whether **to legislate to remove the jurisdiction of the courts to hear Norwich Pharmacal applications against a government department or any other public body.** This would meet the Government's

23 In particular sections 23 and 24 of the Freedom of Information Act 2000, and section 28 of the Data Protection Act 1998.

objective of protecting sensitive material from disclosure and a claimant who wished to obtain information from a public body would still be able to make an application under the Freedom of Information Act 2000 or the Data Protection Act 1998 in the usual way. However, it is the Government's view that such an approach would be a disproportionate response. There are situations in which the operation of the Norwich Pharmacal regime against a public authority raises no real sensitive issues. Accordingly, the Government takes the view that while this reform option would meet the aim of protecting sensitive government material from disclosure, it would go too far in preventing Norwich Pharmacal applications in other cases against Government in which non-sensitive material is at stake.

2.91 An alternative, more focused, option would be **to legislate to remove the jurisdiction of the courts to hear Norwich Pharmacal applications where disclosure of the material in question would cause damage to the public interest.** Under this option, it is envisaged that for material held by or originated from one of the Agencies there would be an absolute exemption from disclosure. It is envisaged that in respect of non-Agency government material where disclosure would cause damage to the public interest if disclosed (for example, for international relations reasons), there would be an exemption from disclosure which would be based on a Ministerial Certificate.

2.92 In this model, if the exemption were raised by the Government on the basis that the material is Agency-held or originated, that would be the end of the proceedings and the Norwich Pharmacal application would be dismissed by the court. If the Minister signs a certificate to say that the material, while not being Agency-held or originated, would nonetheless cause damage to the public interest if disclosed, then that would also bring an end to the proceedings unless the claimant wished to challenge that decision, which they would be able to do on judicial review principles. The Government envisages that those parts of any such review addressing the nature of the sensitive material and the damage caused by disclosure would need to be held in closed session via a CMP.

2.93 The Government sees clear benefits to a proposal along these lines. The proposal is tailored to problematic Norwich Pharmacal applications where disclosure would cause damage to national security or another public interest, leaving the rest of the jurisdiction unaffected. The proposal is also consistent with the approach to national security adopted by Parliament in, for example, the Freedom of Information Act 2000. The Government **seeks views on the viability of such a proposal.**

2.94 An alternative reform option is **to legislate to provide more detail as to what will in future be required to satisfy each of the five elements of the Norwich Pharmacal test.** Seeking to define key terminology in legislation should lead to greater certainty in Norwich Pharmacal hearings and potentially, therefore, less protracted resource-intensive litigation and a reduction in the risk of damaging disclosure. The Government sees benefit in providing the court with a tighter framework when considering the various elements of the Norwich Pharmacal test and **the Government therefore seeks public views on this option.**

2.95 It would of course be possible not to seek to introduce new legislation to address the challenge posed by court-ordered disclosure of sensitive material into foreign legal proceedings, and instead for the Government to continue to defend such applications on a case-by-case basis. If CMPs were statutorily available, the Government would have more confidence that it could defend the application more thoroughly and robustly in a court that could adequately protect the material in question. This may lead to a more effective hearing – a better basis on which a judge may reach a decision.

2.96 However, the Government believes that the risks of such an approach outweigh the limited benefits. Continuing to grapple with the risk of sensitive disclosure overseas will reinforce the concern of foreign intelligence partners that the UK Government cannot safeguard their most sensitive material with any confidence. The UK courts will remain a forum of choice for speculative applicants, and Norwich Pharmacal applications for sensitive material will continue to have a disproportionate impact on the Government, primarily in terms of the risk to

national security caused by disclosure and the expenditure of diplomatic capital in minimising the damage caused to international relationships. Accordingly, the Government would prefer to legislate to clarify how these principles should apply in the national security context.

2.97 These are extremely difficult issues, not least given that the cases in which these issues have arisen have often occurred in circumstances where individuals are facing severe consequences for their liberty.

**Question: What role should UK courts play in determining the requirement for disclosure of sensitive material, especially for the purposes of proceedings overseas?**

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

## Chapter 3

# Non-judicial oversight: proposals and consultation questions

3.1 The courts play a crucial role in scrutinising matters of national security and the activity of the Agencies and the wider intelligence community. There are a number of other bodies responsible for ensuring that there is complementary independent oversight of this area of government activity. In considering the role of these oversight bodies, as with the courts, we must strike a balance between the transparency that accountability normally requires, and the secrecy that security demands.

3.2 Oversight of government has a number of different purposes. These include: improving the effectiveness of the bodies being overseen; detecting and preventing poor administration, waste, abuse and arbitrary behaviour; ensuring that organisations act within their legal boundaries; informing the public of their findings. Oversight typically involves the collection and consideration of evidence, the making of judgements and recommendations based on that evidence and the communication of those conclusions to the Executive, the general public and the bodies being overseen. Oversight must **be effective**, but it also must be **seen to be effective – in other words credible** in the eyes of Parliament and the general public.

3.3 Since the Intelligence Services Act 1994 (ISA) and the Regulation of Investigatory Powers Act 2000 (RIPA) which established the framework for oversight of the Agencies, there have been significant changes in the context in which the Agencies work and in the nature of their work. There have been revolutionary changes in information technology and in the ways in which people communicate. Cyber security is now a high

priority for the UK. There has been a series of events – 11 September 2001, the armed conflicts in Afghanistan and Iraq, the 7 July 2005 London bombings, the Arab Spring – with far-reaching implications for our foreign and security policies. The Agencies now have a more public profile and increased budgets in order to carry out their essential work. The requirement for strengthening the oversight arrangements for the Agencies has therefore grown.

3.4 The Government recognises the criticisms that have been made about current oversight arrangements, particularly that they do not provide sufficient public reassurance that current scrutiny is effective. This Green Paper makes proposals for the development of intelligence oversight arrangements. These are consistent with the proposals that address the need for sensitive material to be safeguarded in civil judicial proceedings.

3.5 Any reforms to the oversight system must not damage national security or impair operational effectiveness. The Agencies operate covertly and their activities and material are necessarily secret. Therefore much of the activity of oversight, given the sensitive nature of the material involved, must also be secret. This condition should not prevent oversight being effective and working well. However, there is a significant challenge involved in deciding how to make public details of the oversight process while at the same time ensuring that material is not released that would damage national security.

3.6 The present framework has built up over time. As the environment in which the Agencies

have operated has changed, and the investigative techniques which they use have developed, some gaps have emerged in the system of oversight. These gaps have been filled in an ad hoc way through Ministerial-approved but non-statutory additions to the remits of current oversight bodies. Another aim of reform, therefore, is to ensure that the system is coherent and robust but also sufficiently flexible to cope with future changes to the global and technological environments and any changes in how the Agencies operate.

3.7 The non-judicial oversight of government departments and associated public bodies generally involves a balance between oversight provided by Parliament and oversight provided by other bodies. In the case of the intelligence community, the key existing oversight bodies are the Intelligence and Security Committee (ISC), the Intelligence Services Commissioner and the Interception of Communications Commissioner as well as the Investigatory Powers Tribunal.

3.8 All these oversight bodies provide robust challenges to, and scrutiny of, the work of the intelligence community. The ISC, for instance, has investigated and produced special reports on the London terrorist attacks on 7 July 2005 and rendition. The Commissioners regularly monitor and audit the use of the Agencies' intrusive powers and outline their findings in annual reports.

3.9 In considering options for reform, the Government is determined to ensure the right balance of oversight: the framework should work as a cohesive whole, with different bodies playing the roles for which they have the appropriate expertise. Some choices are drawn out in the consultation questions below.

### Ministerial responsibility and oversight

3.10 The Prime Minister has overall responsibility within government for intelligence and security matters and for the Agencies. Day-to-day Ministerial responsibility for the Security Service lies with the Home Secretary and for the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ) with the Foreign Secretary. The Home Secretary is

accountable to Parliament, and therefore to the public, for the work of the Security Service; the Foreign Secretary has the same accountability for SIS and GCHQ. They each have a close knowledge of the work of the Agencies and personally authorise warrants under ISA and RIPA, and in some circumstances are responsible for authorising specific Agency operations.

3.11 The Heads of Agencies have a formal requirement to report to Ministers. Each Agency Head has a separate statutory requirement to make an annual report on the work of their organisations to the Prime Minister and the relevant Secretary of State and may at any time report to either of them on any matter relating to their work. However, the Agency Heads have a statutory responsibility for the operational work of their Agencies and are operationally independent from Ministers.

### Independent parliamentary oversight

3.12 The ISC is a unique committee of Parliamentarians drawn from both Houses of Parliament. It was set up under statute and reports to the Prime Minister. It oversees the expenditure, administration and policy of the three Agencies. The ISC's remit is in line with that of a departmental select committee. However, in order to give it safe access to secret intelligence material there are a number of safeguards regarding its reporting and appointment arrangements that differ from select committee procedures.

3.13 These arrangements were reviewed as recently as 2007 when *The Governance of Britain* Green Paper made a series of reform proposals aimed at bringing the ISC as far as possible into line with other select committees, while maintaining the necessary arrangements for safeguarding sensitive material. These proposals were: an increased role for Parliament in the appointment process for members of the ISC; some hearings of the ISC to be structured to allow unclassified evidence to be heard in open session; providing the Committee with additional support in order to enhance its abilities to conduct investigations; finding alternative, secure accommodation outside the offices of the Cabinet Secretariat; and the ISC

Chairman opening debates on its reports in the House, rather than a Government Minister. All of these proposals have now been implemented with the exception of evidence being heard in open session.<sup>1</sup>

For more detail on the ISC, see Appendix H.

3.14 However, there continues to be criticism of the ISC. These criticisms focus on the fact that it is separate and different from other parliamentary committees, that it answers to the Prime Minister, that it is insufficiently independent, that it does not have sufficient knowledge of the operational work of the Agencies and that the process by which the ISC is appointed, operates and reports is insufficiently transparent.

3.15 The current ISC has itself developed and put forward proposals for reform and has communicated these proposals to the Government in advance of this Green Paper. The ISC summarised the key principles on which its proposals are based in its 2010–11 Annual Report as follows:

- ♦ the Intelligence and Security Committee should become a Committee of Parliament, with the necessary safeguards, reporting both to Parliament and the Prime Minister
- ♦ the remit of the Committee must reflect the fact that the ISC has for some years taken evidence from, and made recommendations regarding, the wider intelligence community, and not just SIS, GCHQ and the Security Service
- ♦ the Committee's remit must reflect the fact that the Committee is not limited to examining policy, administration and finances, but encompasses all the work of the Agencies
- ♦ the Committee must have the power to require information to be provided. Any power to withhold information should be held at Secretary of State level, and not by the Heads of the Agencies
- ♦ the Committee should have greater investigative and research resources at its disposal.

3.16 The Government agrees with the current ISC that there are serious reforms that could be made to the Committee's status, powers and remit that could enhance public confidence in the scrutiny of intelligence activity. The Government is committed to giving effect to these improvements, subject to the outcome of this consultation, including on the broad range of options for oversight reform, and subject to agreeing with the current Committee the details of how the new system can best work.

#### Status of the ISC

3.17 A key question for reform, therefore, is whether the ISC's status can be changed, to strengthen its links to Parliament, while retaining the appropriate safeguards that ensure it has access to the sensitive information it needs.

3.18 A possible option would be to change the status of the ISC to that of a departmental **select committee**. Departmental select committees have a remit 'to examine the expenditure, administration and policy' of the relevant government department and associated public bodies. A Standing Order, which would need to be renewed each Parliament, could cover appropriate handling of sensitive material, accommodation, staffing and reporting. Creating a select committee would result in oversight being demonstrably undertaken by Parliament.

3.19 However, under such arrangements the Government would clearly have no veto on publication of sensitive material. There would be a real risk that, with fewer safeguards in place than under the present arrangements, Agency Heads would find it hard to reconcile their statutory duty to protect information with their statutory duty to facilitate parliamentary oversight. Sharing of less sensitive information and a corresponding reduction in both the credibility and effectiveness of the oversight the committee provided could be the result. **For these reasons, the Government believes this option should not be taken forward.**

3.20 The Government has considered the ISC's own proposal that it becomes a **statutory Committee of Parliament**, reporting formally to Parliament alongside its existing reporting

<sup>1</sup> See paragraph 3.35 for more detail.



arrangements to the Prime Minister. This change would be significant. It would result in the Committee being demonstrably accountable to Parliament. In contrast to the select committee proposal, this change in status would be statutory and would therefore allow appropriate and enduring safeguards to be put in place (some of which are explored below) to ensure the protection of sensitive material. **The Government proposes that this option is pursued.**

#### Remit of the ISC

3.21 The ISC has a broad, and in practice flexible, statutory remit that covers examination of the 'expenditure, administration and policy' of the Agencies. In some of its previous reports and inquiries, and in order to be able to fulfil its remit effectively, the ISC has also undertaken work that has involved some access to past operational material. The clearest example of this was the ISC's report into the 7 July 2005 terrorist attacks.

3.22 This ability to look at the operational work of the Agencies where it is relevant to the particular nature of the inquiry has been used effectively and constructively by the ISC in the past. For that reason the Government is giving careful consideration to the **ISC's proposal to extend its remit to include operational aspects** of the work of the Agencies. The consequences of creating such a general power are significant and need careful thought to ensure that the implications have been understood. The principles that the Government believes are important in considering this issue include safeguarding the integrity of Ministerial responsibilities, avoiding overlap with the roles of other independent oversight bodies and ensuring that there is no lessening of the effectiveness of the working of the Agencies or undue resource burden placed upon them. In addition, any such oversight of operational work would need to be clearly retrospective and in the Government's view would need to be focused on matters of significant national interest. Any change of this kind would therefore need to be based on a clear understanding between the Government and the Committee on how this should work in practice, articulated either in legislation or, possibly, a supporting document such as a Memorandum of Understanding.

3.23 As the ISC has developed its role it has, with the agreement of previous and current governments, **taken evidence from bodies beyond the three Agencies** which are a part of the wider intelligence community within government. These include Defence Intelligence in the Ministry of Defence (MOD), the Office for Security and Counter-Terrorism in the Home Office and the central government intelligence machinery in the Cabinet Office (including the Joint Intelligence Organisation). It has also, in its annual reports, made recommendations relating to those bodies. The ISC has proposed that this role should be formalised.

3.24 These bodies are part of larger departments (MOD, Cabinet Office and Home Office) which are overseen by the appropriate departmental select committee. However, where the work of these organisations relates directly to intelligence material, the relevant departmental select committees are not able to provide oversight. **The Government proposes formally to recognise the wider role the ISC should play in overseeing the Government's intelligence activities by enabling it to take evidence from any department or body in the wider intelligence community** about intelligence-related activity where to do so would help the ISC provides coherent intelligence oversight. This development would not affect the primary accountability of those bodies to the relevant departmental select committee of the House of Commons.

#### Procedural and practical improvements to the ISC

##### Appointments to the Committee

3.25 The ISA specifies that Committee members are to be appointed by the Prime Minister in consultation with the Leader of the Opposition. Within that context, new processes for making appointments to the ISC were adopted by the two Houses of Parliament following the 2007 *Governance of Britain* Green Paper. This change resulted in, for the Commons, the Committee of Selection being permitted to propose nominations for the ISC; and, for the Lords, nominations being agreed through 'the usual channels'. The names

are agreed by the House before being sent to the Prime Minister to make the final appointments in consultation with the Leader of the Opposition. The Prime Minister nominates and appoints the Chair of the ISC, after consulting the Leader of the Opposition. The parliamentary process is not binding on the Prime Minister, who is free to reject the House's recommendation, or to appoint members to the ISC without a recommendation from the House at all.

3.26 The Government has looked at whether additional reforms could be made to further normalise ISC appointments, recognising that ensuring that the appointments process is as independent as possible strengthens the credibility of the Committee. In doing so we have had to be conscious of the need to retain some safeguards with regard to appointments: membership of the ISC confers access to highly sensitive information, disclosure of which could lead to damage to national security. It is important that any appointments process manages that risk.

3.27 The approach preferred by the ISC is that Parliament and not the Prime Minister should, in future, make the final decision on membership and the Chair of the ISC. This would not be unusual in the House of Commons where important committees such as the Standards and Privileges Committee have their membership chosen in this way. The names of proposed members of the Committee are put on the Order Paper but the House of Commons can reject them if it so wishes until it is satisfied as to the final membership.

3.28 Alternatively, the Government has considered adoption of the Reform of the House of Commons Committee (known as the Wright Committee<sup>2</sup>) proposals. Wright proposed that ISC membership nominees be elected by secret ballot from within party groups, that the Chairman should be held by convention by a member of the majority party and should be elected by a secret ballot of the whole House of Commons with a process for the Prime Minister to pre-approve any individuals wishing to stand.

3.29 In both these options Parliament would have the final word on the make-up of the ISC. In the ISC's preferred approach this would be expressed through an ability to reject the proposed membership. In the Wright Committee proposals Parliament would select the membership by vote from a list of candidates.

3.30 The Wright Committee's proposals, however, did not take into account that the ISC is a Joint Committee of the House of Commons and the House of Lords. The nearest current equivalent is the Joint Committee on the National Security Strategy whose membership, as with other Joint Committees, is determined on the same basis as is recommended by the ISC as regards its future membership.

#### Accommodation, staffing and budget

3.31 We are considering possible changes to the ISC's staffing, accommodation and funding with a view to strengthening both the ISC's actual and symbolic connection to Parliament. The most tangible physical demonstration of independence, and a natural consequence of the ISC becoming a Committee of Parliament, would be **to make arrangements with the parliamentary authorities for the ISC to be accommodated in suitably secure premises on the parliamentary estate, rather than on the government estate. Similarly, its staff could have the status of parliamentary staff** (rather than departmental civil servants based in the Cabinet Office), and **its budget funded directly from parliamentary appropriation** rather than the Cabinet Office's departmental budget.

3.32 The Government accepts that some of the proposals in this section, if implemented, would require a modest uplift in the Committee's current levels of resourcing. The ISC itself has made a case for an increase in its resourcing. Following decisions on next steps after this consultation, the Government – with the parliamentary authorities if the above plans are taken forward – **proposes to review the level of resourcing that the ISC requires to support it in the discharge**

2 The Wright Committee was appointed on 20 July 2009 to consider and report on four identified matters: the appointment of members and chairs of select committees; the appointment of the Chairman and Deputy Chairmen of Ways and Means; scheduling business in the House; enabling the public to initiate debates and proceedings in the House.

**of its functions and the nature of the skills the Committee requires to have at its disposal.**

#### Production and publication of reports

3.33 The ISC deals with sensitive national security material and it is necessary that appropriate protection is given to that material especially with regard to publication of reports and papers. Not all of the ISC's work can be made public. The ISA prescribes how some aspects of ISC reporting should be handled; other practices have developed over time.

3.34 However decisions on publishable material are reached, it is important that the ISC does publish whatever is safe to publish in a form that is accessible to the general public. As much of the work of the Committee necessarily takes place in private, producing credible and accessible public reports is particularly important to give Parliament and the wider public reassurance that the Committee provides effective oversight.

#### Public evidence sessions

3.35 In order to fulfil its remit effectively, which requires it to have access to sensitive material, the ISC's meetings will still have to, as a rule, take place in private. However, as part of the *Governance of Britain* reforms, the Government committed to work with the ISC to provide **public evidence sessions** where this can be achieved without compromising national security or the safety of individuals. Previous Committees have chosen not to take this idea forward but **both the Government and the current ISC are committed to making this concept work.**

#### Access to information

3.36 Under current legislation the ISC requests information from the Heads of the three Agencies who can, in theory, decline to disclose information if it is 'sensitive' (as defined by ISA – which could include information about sources or methods or relating to particular operations or which has been provided by foreign partners who do not consent to its onward disclosure). An Agency Head's refusal to disclose such information to the ISC can be overturned by the relevant Secretary of State on public interest grounds. In practice,

Agency Heads have rarely refused an ISC request for information. The Government agrees with the ISC's proposal that the **Committee should be given the power to require information from the intelligence Agencies.** The Government also agrees with the ISC proposal that **this should be subject only to a veto exercisable by the relevant Secretary of State,** rather than by the Head of the individual Agency, as now.

3.37 In practice, the ISC, in common with departmental select committees, takes most of its evidence in the form of face-to-face sessions (in the case of the ISC with Ministers, Agency Heads and, where appropriate, senior officials) or in the form of prepared written material provided in response to specific requests for written evidence. The Government expects that this will be how the ISC will, in general, continue to operate but we recognise that the ISC will, depending on the nature of its inquiries, sometimes need to be able to access primary material. In such cases, the ISC will need to work with the Agencies or department in question to agree practical ways to manage the sharing of information.

3.38 The Government is keen to hear views on the various proposals for reforming parliamentary oversight. The Government itself supports most of the ISC's proposals for changing its status, remit and powers. Other proposals, most notably that which concerns oversight of operational work, will require very careful consideration for the reasons outlined above.

*Question: What changes to the ISC could best improve the effectiveness and credibility of the Committee in overseeing the Government's intelligence activities?*

## The Commissioners

### The role of the Commissioners in intelligence oversight

3.39 Independent oversight of the Agencies is provided by the Intelligence Services Commissioner and the Interception of

Communications Commissioner. The Commissioners are appointed by the Prime Minister for a (renewable) period of three years and must hold or have held high judicial office. The Intelligence Services Commissioner's central function is to keep under review the issue of warrants by the Secretary of State, including those authorising intrusive surveillance (e.g. eavesdropping) and interference with property, in order to make sure that the Secretary of State's issue of the warrants was in compliance with legal requirements. The Interception of Communications Commissioner's central function is to keep under review the issue of warrants for the interception of communications. More details of the remits of the Commissioners can be found at Appendix G.

3.40 The Commissioners report to the Prime Minister and these reports are published and laid before Parliament. Certain information is excluded from the public report if it appears to the Prime Minister, after consultation with the relevant Commissioner, that publication of that information would be contrary to the public interest or prejudicial to national security, to the prevention or detection of serious crime, to the economic well-being of the UK, or to the continued discharge of the functions of any public authority whose activities are subject to the Commissioners' review. The practice of both Commissioners has therefore been to write the Report in two parts, one of which is a Confidential Annex that is not published.

3.41 The Commissioners provide assurance and challenge to Ministers and Heads of Agencies on the legality and proper performance of the activities of the Agencies. They advise on how Agencies can enhance their compliance with statutory obligations and ensure that new and existing capabilities are developed and used lawfully, proportionately and only where necessary. As such they provide advice of real practical and operational value and their role is therefore different from, and their work is complementary to, that of the ISC.

#### The remit of the Commissioners

3.42 The Commissioners' existing statutory remits are focused on monitoring compliance

by the Agencies with the legal requirements in the exercise of their intrusive powers.

The Government has occasionally asked the Commissioners to take on additional duties outside that remit. These have typically required an ongoing role in monitoring compliance with new policies or an intensive health check on a particular work area. Most recently, for example, the Intelligence Services Commissioner was invited by the Prime Minister to monitor the Agencies' compliance with the *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*.

3.43 The Government proposes that the Commissioners' ability to discharge these types of duties is placed on a statutory footing, in order to ensure transparency, coherence and a clear basis of authority. This would need to be broad enough to cover current non-statutory duties and also a range of potential future duties. **The Government proposes that this is done by adding a general responsibility for overseeing the effectiveness of operational policies to the statutory remit of the Intelligence Services Commissioner, who would maintain responsibility for monitoring compliance by the Agencies with the necessary legal requirements in the exercise of their intrusive powers.** The specific areas on which the Commissioner focuses at any one time would need to be agreed, on an ongoing basis, with the appropriate Secretary of State.

3.44 The effectiveness and value of the Commissioners in providing assurance and challenge to Ministers is not in doubt. They are highly respected former members of the judiciary whose experience and insight is invaluable in checking the necessity and proportionality of the use of the Agencies' intrusive powers. However, their low public profile means that they play a lesser role in providing assurance to the general public that the activities of the Agencies are at all times reasonable, proportionate, necessary and compliant with all legal obligations. A number of steps have been taken recently to **increase the public profile of the Commissioners**. The Commissioners' most recent annual reports have

been revised to make them more readable and with the inclusion of more qualitative information of potential interest to readers. A new dedicated website for the Commissioners has been established and is expected to go-live around the time of publication of this Paper. These steps are important as they allow the Commissioners to explain to the public how their offices work, what they do and how they link into other elements of the oversight landscape. The Government considers that future appointments should bear in mind the importance of the public element of the Commissioner role.

### The Inspector-General model

3.45 In other jurisdictions, such as Australia, non-parliamentary independent oversight of security and intelligence agencies is undertaken by one single body. Such bodies are often known as Inspectors-General and usually have oversight of all of the Agencies' covert investigative techniques. However, their functions also tend to be broader than providing legal scrutiny and are more closely akin to those of an ombudsman with a regulatory function. Inspectors-General tend to have a more public-facing role, explicitly tasked to explain what they do and how they hold the Agencies to account, and also provide a response to public interest in, and criticism of, intelligence activity. In this way they are able to provide public assurance that the activities of the Agencies are at all times reasonable, proportionate, necessary and compliant with all legal obligations.

3.46 In the UK, an Inspector-General would differ from our current system in that more oversight functions would be concentrated in one body rather than split between different bodies with specific areas of expertise (although the ISC would continue to exist to provide separate parliamentary oversight). Having these functions carried out by one body carries the risk that the nominated Inspector-General can develop a more political relationship with government and thus potentially seem to provide less independent advice than, for example, the Commissioners do currently. This risk could be mitigated by a rigorous and open appointments process. The potential advantage, however, in having non-parliamentary independent oversight functions concentrated in a single public-

facing body is that the oversight system would work more transparently, be easier to understand and therefore have more public credibility.

3.47 Importing such a model into the UK system would require a major overhaul of the current Commissioner arrangements. It would also need to be managed in such a way that its remit did not overlap with that of the ISC. The Government is looking carefully at whether the benefits of such a major change would outweigh the costs. There are a number of different approaches that could be taken if a decision were taken to **create an Inspector-General**. One approach would be for the Inspector-General to be responsible for the oversight of all of the Agencies' covert investigative techniques, effectively subsuming the current roles of the Intelligence Services Commissioner and of the Interception of Communications Commissioner as they relate to the Agencies. Potentially, other functions not currently undertaken by either Commissioner could also be added to the remit, for example the ability to oversee the operational work of the Agencies.

3.48 A consequence of this approach would be to have an Inspector-General whose remit includes responsibility for oversight of Agency interception and another body responsible for non-Agency interception. This approach brings the risk that the two bodies would take different approaches to the oversight of interception and interpretation of the law, in a context of complex and rapidly evolving communications technology, and so the standards and practices of interception relating to the Agencies and non-Agency bodies could diverge. An alternative approach therefore would be for an Inspector-General to have responsibility for oversight of all interception, including by non-Agency bodies.

3.49 For illustrative purposes only, one potential model for an Inspector-General is set out at Appendix I.

*Question: What changes to the Commissioners' existing remit can best enhance the valuable role they play in intelligence oversight and ensure that their role will continue to be effective for the future? How can their role be made more public facing?*

**Question: Are more far-reaching intelligence oversight reform proposals preferable, for instance through the creation of an Inspector-General?**

### Ensuring a balanced system

3.50 The Government is committed to ensuring that any reforms achieve balance in the overall system and are sensitive to the potential for overlap between independent oversight provided by parliamentary and other independent bodies. The areas of greatest risk are likely to be oversight of operational policy and of operational activity more broadly. Any set of reforms should ensure that the functions and activity of the body or bodies responsible for independent oversight overlap as little as possible and that the appropriate functions are performed by the body most suited to that role. The same considerations are relevant in considering which bodies, existing or new, could be best positioned to enhance public understanding of and confidence in intelligence oversight. The Government would expect that the relevant independent oversight bodies might, as part of their existing functions, seek to periodically consider the effectiveness of any new closed material procedures arising from this Green Paper.

3.51 The Government's view is that some of the proposals considered above are incompatible with each other were they both (or all) brought forward together, both from the perspective of managing potential areas of overlap and from the equally important objective of ensuring the overall impact of oversight activity is proportionate and does not undermine the primary business of national security. So, for example, if a decision was made to have a parliamentary committee with significantly enhanced powers of oversight, particularly with regard to operational activity, then it would be inappropriate also to create a powerful Inspector-General. Equally, if a decision was taken to create an Inspector-General then it would be inappropriate to significantly increase the remit of the ISC, with particular regard to oversight of operational activity.

3.52 However, the Government believes that most of the reform proposals that the ISC has made, and which it supports, can be made regardless of the approach taken on the appropriate balance between independent oversight carried out by parliamentary and other independent bodies. These would include: making the ISC a Committee of Parliament; reforms relating to appointments; the ISC's accommodation, staffing and budget; the power to require information, with a veto resting with the relevant Secretary of State; and formalisation of the ISC's remit with regard to the wider intelligence community.

3.53 The Government is therefore keen to hear views on the issue of balance between the different elements of the oversight system. Assumptions that should be tested as these questions are considered include whether it is right to assume Parliamentarians will generally be better placed than other independent figures to engage with the general public and whether legal experts will generally be better placed to undertake detailed compliance monitoring?

**Question: What combination of existing or reformed arrangements can best ensure credible, effective and flexible independent oversight of the activities of the intelligence community in order to meet the national security challenges of today and of the future?**

**Question: With the aim of achieving the right balance in the intelligence oversight system overall, what is the right emphasis between reform of parliamentary oversight and other independent oversight?**

## Appendix A

# Secret intelligence, diplomacy and protecting the public

1. The National Security Strategy refers to the vital role that the security and intelligence agencies (the 'Agencies'), together with the intelligence gathering arms of the police and armed forces, play in delivering that strategy:

*to use all our national capabilities to build Britain's prosperity, extend our nation's influence in the world and strengthen our security...We will use all the instruments of national power to prevent conflict and avert threats beyond our shores: our Embassies and High Commissions worldwide, our international development programme, our intelligence services, our defence diplomacy and our cultural assets.*

2. Our Agencies do this work diligently and tirelessly 24 hours a day throughout the world; their work involves identifying, and containing and disrupting threats, investigating targets, recruiting and debriefing sources to inform this work, and providing assessments. They gather key secret information which enables the Government to stay one step ahead of those who would harm our security and our way of life. They gather this information by working with each other on an inter-Agency basis, through key intelligence sharing relationships with foreign partners and by working with domestic partners such as the police to deliver national security outcomes. An ability to protect and safeguard secret information and its sourcing is essential to their effectiveness. Their work requires the highest moral and ethical standards, aspects which are engrained in the Agencies' ethos.

3. Confidence in the integrity of the staff of the Agencies is paramount because they are required

to work covertly and out of the public eye. It is inherent in their work that most of it has to be done in secret in order to protect those who risk their lives for our security, to maintain the confidence and co-operation of partners overseas and to protect sensitive techniques, capabilities and relationships on which future security depends.

4. Secret intelligence allows the Government to monitor individuals, networks and events that pose a threat to national security and the economic well-being of the country. Secret intelligence is information obtained about individuals, groups or states without their knowledge. It may be acquired in many different ways, such as through the debriefing of human sources, interception of communications (for example telephone or email), or surveillance (both human and technical).

5. The UK is demonstrably a safer place as a result of the intelligence collected by the Agencies; governments have a right to use covert means to obtain intelligence in order to protect their citizens and defend their liberties.

6. Protection of intelligence sources is of paramount importance, never more so than in the case of human sources (also known as 'agents') – not only do the Agencies have legal obligations as well as fiduciary duties of care in this area, but the intelligence that flows from human source reporting is essential to the Agencies' operational effectiveness and is thereby essential to the protection of national security. The confidence of agents in the Agencies' ability to protect their identity is vital to the ongoing relationship and provision of information. Should that confidence be broken or eroded in any way, this will have a

serious deterrent or inhibitory effect on agent recruitment and retention, which in turn will have serious adverse consequences for the future flow of human intelligence, the Agencies' operational effectiveness and the protection of national security.

7. It is also vitally important to protect the secrecy of operations and investigations. If a hostile individual or group – for example a foreign intelligence service or terrorist group – were to become aware that they were the subject of interest to the Agencies, they could not only take steps to thwart any (covert) investigation or operation but also attempt to discover, and perhaps reveal publicly, the methods or techniques used or the identities of the officers or agents involved. Compromise of sources, methods, techniques or personnel affects both the individual investigation or operation and potentially all others, as the risk of deploying such sources, methods, techniques and personnel is increased.

8. Conversely, if a hostile individual or group were to become aware that they were not the subject of Agency interest, they would then know that they could engage or continue to engage in their activities with increased vigour and increased confidence that they will not be detected. So it is vitally important to protect the limit or the extent of the Agencies' coverage and capability. This is why Agencies have long relied on the principle of **'neither confirm nor deny'**.

### The role of the Diplomatic Service

9. Other areas of government activity also generate sensitive material, the protection of which is vital to the national interest. One such area is the conduct of the UK's diplomatic relations with other states and international organisations such as the United Nations and the European Union. Diplomatic relations cover a range of government business, including co-operation on issues such as trade and finance, energy, human rights, counter-terrorism and security policy. The transnational nature of these issues means that the UK is not able to respond to them alone, but must work with and through bilateral partners, i.e. other states and international organisations. In order for the UK to influence the international approach on

these and other issues, it must build and nurture relationships based on mutual trust and confidence with a wide range of partners, as a basis for frank dialogue and co-ordinated action.

10. The Government's ability to engage in this frank dialogue with other governments is built wholly on these partners' confidence that information they choose to share with the UK, which may for legitimate reasons not be in the public domain, will be treated in confidence, and the UK has a similar expectation of how other governments will treat information we choose to share with them. A loss of confidence in the UK's ability to protect sensitive diplomatic reporting would result in a gradual erosion of the Government's ability to gather the information and promote the sort of co-operation, through its diplomatic relations, that is essential to protect national security and promote the wider national interest.

11. Although the practical effect of any disclosure of sensitive information shared with the UK on diplomatic channels by another state is highly case specific, in the event of a failure to protect such information, the result is likely to be not merely embarrassment but potentially a real loss of trust and confidence by an international partner, which could overshadow diplomatic relations and adversely affect practical co-operation on important issues for some time. This could put the UK in a fundamentally weaker position – lacking the access to critical information and relationships, and correspondingly less able to influence – in protecting national security and promoting the wider national interest.



## Appendix B

# Public Interest Immunity

1. Public Interest Immunity (PII) is a mechanism for handling disclosure of sensitive information in litigation.
2. The courts have long recognised that evidence, while relevant to the issues between the parties in a case, must be excluded if the public interest in withholding the information outweighs the public interest in disclosing it. This involves the court balancing competing aspects of the public interest: the public interest in the non-disclosure of certain documents and the public interest in open justice. PII is a common law principle – that is to say, it has been established and developed through case law.
3. It used to be accepted that documents falling within a certain class of documents, such as

Cabinet documents, were immune from disclosure on that basis. However, since the statements made to Parliament by the Attorney General and the Lord Chancellor,<sup>1</sup> Ministers have focused directly on the damage which would be caused by disclosure and now claim PII only where the disclosure of the content of the document would cause real damage or harm to the public interest.

4. The areas of public interest which may be protected by PII include national security, international relations, and the prevention or detection of crime. The categories of PII are not fixed.<sup>2</sup> However, the courts will not recognise new classes of immunity without clear and compelling evidence.<sup>3</sup>

<sup>1</sup> HC Debate 18 December 1996, cols 207 (CG49–50) and 157 HL, Official Report (5th Series) 18 December 1996, cols 1507–17. Note that these statements relate only to the operation of PII in England and Wales.

<sup>2</sup> Lord Hailsham remarked in *D v NSPCC* [1978] 2 All ER 589 that 'the categories of public interest are not closed, and must alter from time to time whether by restriction or extension as social conditions and social legislation develop'.

<sup>3</sup> *R v Chief Constable, West Midlands ex p Wiley* [1995] 1 AC 274

## Appendix C

### Closed material procedures

1. A closed material procedure (CMP), which involves the use of Special Advocates, is a procedure in which relevant material in a case, the disclosure of which would harm the public interest ('closed material'), can still be considered in the proceedings rather than being excluded as with PII.

2. It is designed to provide individuals with a substantial measure of procedural justice in the difficult circumstances where, in the public interest, material cannot be disclosed to them. It is therefore a mechanism for seeking to reconcile the public interest in open justice and the public interest in safeguarding national security.

3. The starting point in such proceedings is that the individual is given as much material as possible, subject only to legitimate public interest concerns. The disclosure process is designed to achieve this.

4. Proceedings have both 'open' and 'closed' elements. All the material – open and closed – that the Government relies upon in its case is laid before the court and the Special Advocate. The individual concerned and his legal representatives can be present at the open hearings, and see all the open material used in those hearings. They cannot be present at the closed parts of the proceedings, or see the closed material. The Special Advocate attends all parts of the proceedings, and sees all the material, including the closed material not disclosed to the individual. He can take instructions from the individual before he reads the closed material, and written instructions after he has seen the closed material. A Special

Advocate can also communicate with the individual after he has seen the material, provided it is with the permission of the court.

5. A Special Advocate is a security cleared barrister/advocate in independent practice who also receives special training for their role. The role of the Special Advocate is to act in the individual's interests in relation to closed material and closed hearings – although they do not act for the individual, nor is the individual their client.

6. Part of the function of Special Advocates is to ensure that the closed material is subject to independent scrutiny and adversarial challenge – including making submissions (in closed session) on whether or not the closed material should in fact be disclosed to the individual. Special Advocates can argue, and have successfully argued, that closed material should be disclosed in this way.

7. The judge in the case also has an important role to play in challenging the closed material and weighing the impact that non-disclosure has had on the fairness of the proceedings. It is not the Secretary of State but the court that determines whether or not material should be withheld. The disclosure process is designed to ensure that the maximum amount of material that can be disclosed to the individual without damaging the public interest is disclosed.

8. A CMP was first introduced in the context of immigration deportation decisions. Following the case of *Chahal v United Kingdom*,<sup>1</sup> the European Court of Human Rights acknowledged

that reliance on confidential material might be unavoidable in cases where national security was at stake. The court cited with approval a system used in Canada which suggested that there could be procedures which 'both accommodate legitimate security concerns about the nature and sources of intelligence information and yet accord the individual a substantial measure of procedural justice'.<sup>2</sup> The Special Immigration Appeals Commission Act 1997 introduced a CMP to remedy the deficiencies in the advisory panel system.

Other circumstances where statute provides for a CMP include:

- ◊ the Proscribed Organisations Appeal Commission
- ◊ proceedings in the Employment Tribunal concerning national security<sup>3</sup>
- ◊ control order cases under the Prevention of Terrorism Act 2005
- ◊ financial restrictions proceedings under the Counter-Terrorism Act 2008
- ◊ the Sentence Review Commission and Parole Commission in Northern Ireland.

## CMPs in Northern Ireland

9. CMPs in Northern Ireland are not unusual and generally take place in the context of prisoner release and recall hearings.

10. The Northern Ireland (Sentences) Act 1998 and associated rules provide for the early release of certain prisoners serving terms of imprisonment in Northern Ireland. Those released can be recalled to prison if they breach their licence conditions. This legislation allows the Secretary of State to certify information as 'damaging' and to present it to the Sentence Review Commissioners, the body which rules on prisoner release. In these circumstances the prisoner is provided with a 'gist' of the damaging information and is represented by a Special Advocate in the closed proceedings.

11. A similar process is provided for in the non-statutory additional safeguards to the Northern Ireland (Remission of Sentences) Act 1995, which allows prisoners convicted of certain offences under the Terrorism Act 2000 to be released on licence halfway through their sentence.

12. The Parole Commissioners' Rules (Northern Ireland) 2009 allow the Secretary of State to introduce 'confidential' information in release and recall cases considered by the Parole Commissioners. Confidential information may also be the basis for a decision by the Secretary of State to revoke a licence. The Special Advocate procedure applies.

2 See [131] of *Chahal v United Kingdom* 23 EHRR 413 (1996)

3 The Employment Tribunal has the power to hear closed information in cases involving Crown employment if it is 'expedient in the interests of national security' (see rule 54 of Schedule 1 to the Employment Tribunals (Constitution and Rules of Procedure) Regulations 2004 (SI.2004/1861)).

## Appendix D

### *AF (No.3)* and the challenges of providing summaries of sensitive material

1. Following the European Court of Human Rights judgment in the case of *A and Others v UK*<sup>1</sup> (which related to the powers under Part 4 of the Anti-terrorism, Crime and Security Act 2001 to detain pending deportation foreign national suspected terrorists, even if deportation was not an option at that time), the House of Lords ruled, in *AF (No.3)*,<sup>2</sup> that for the stringent control orders before them, in order for control order proceedings to be compatible with Article 6, the controlled person must be given sufficient information about the allegations against them to enable them to give effective instructions to the Special Advocate in relation to those allegations. This means that, even where disclosure would be against the public interest (for example if disclosure could put the life of an informant at risk), the disclosure obligation set out in *AF (No.3)* now applies.

2. The Government faces difficult choices as to how best to protect the public interest following the *AF (No.3)* judgment. The Government must balance the importance of protecting the public from the risk of terrorism posed by the individual against the risk of disclosing sensitive material. Disclosing this material potentially reduces the Government's ability to protect the public from the risk of terrorism. Where the disclosure required by the court cannot be made because the potential damage to the public interest is too high, the Government must withdraw the information from the case. If the case cannot be sustained on the remaining material, the court will quash the control order because of this inability to disclose (which allows the individual to claim damages) even where we consider those orders

to be necessary to protect the public from a risk of terrorism. (The judgment caused particular difficulties in relation to control orders already in force at the time of the judgment, which had not been imposed with the new disclosure requirement in mind.) And the Government might not be able to impose a control order at all in a new case where it would otherwise wish to, because it may consider that the disclosure requirement could not be met.

3. Even where cases can be maintained, the Government may have to make damaging disclosure in order for the judge to uphold the order. Since 2009, some individuals have had their control orders revoked (and subsequently quashed) because the Government considered it could not make the disclosure required by *AF (No.3)*. However, other control orders have been upheld by the High Court when considered in light of the requirements of Article 6 following *AF (No.3)*. This demonstrates that the regime remains usable, notwithstanding the problems caused by *AF (No.3)*.

4. The Government has announced that it will be repealing control orders legislation and replacing it with a new system of terrorism prevention and investigation measures (TPIM). The disclosure requirements required by the judgment in *AF (No.3)* will be applied as appropriate by the courts in TPIM proceedings.

5. Since judgment was given in *AF (No.3)*, there has been ongoing litigation about the reach of that judgment to other proceedings that use sensitive material.

1 [2009] ECHR 301

2 [2009] UKHL 28

## Appendix E

### Section 2(2) of the Security Services Act 1989 and sections 2(2) and 4(2) of the Intelligence Services Act 1994

1. The Head of each Agency has a duty to ensure that there are arrangements in place for securing that information is only obtained to the extent necessary for the proper performance of that Agency's functions and that no information is disclosed by that Agency except to the extent that it is necessary:

- » for the proper discharge of its functions
- » in the protection (or in the interests) of national security
- » for the purpose of preventing or detecting serious crime, or
- » for the purpose of any criminal proceedings.

2. Although the wording of section 2(2) of the Security Service Act 1989 and sections 2(2) and 4(2) of the Intelligence Services Act 1994 differ slightly, there is considered to be no material difference between them in their practical operation or effect.

3. The arrangements for which the Head of each Agency is responsible are thus drawn tightly around that Agency's statutory functions, and Parliament has very narrowly drawn the lawful scope for disclosure.

4. Decisions on disclosure covered by these provisions are routinely taken at all levels within an Agency on a day-to-day basis. Important decisions on disclosure, particularly where there are significant legal and/or political implications, are taken at a senior management level, and sometimes by the Head of the Agency.

## Appendix F

### Further analysis on Special Advocates

1. Since Special Advocates were introduced in 1997, various select committees and non-governmental organisations have raised concerns about their operation. Special Advocate arrangements have changed over the years to address many of these concerns – for example, the Special Advocate Support Office was set up, training sessions were introduced and the system for appointing Special Advocates was amended.

2. Many further arguments for change have been made before the courts in litigation, and (excluding the disclosure requirement in some contexts as a result of *A and Others v UK*<sup>1</sup>) the courts have so far not accepted that changes to the system need to be made in order for it to be compliant with the European Convention on Human Rights (ECHR). However, in light of our consideration of extending the use of closed material procedures (CMPs), we have looked again at many of these concerns. A principal concern relates to the limitations on communication between the Special Advocate and the individual after they have seen the closed material. This is addressed in the main body of this Green Paper (see paragraphs 2.28–2.36). Other concerns include:

#### Reporting of closed judgments

3. In cases involving sensitive material, the judge is under a duty to put as much of his judgment into open court as possible, including statements of legal principle that are most likely to have cross-case relevance. However, there may be the need for a closed judgment. These judgments contain highly sensitive material and so cannot be openly published. Special Advocates are able to make requests to see closed judgments relevant to their case. However, concerns have been raised that Special Advocates face difficulties in establishing whether or not closed judgments relevant to their work have been handed down by the courts. As recommended in the Review of Counter-Terrorism and Security Powers, the Home Office is taking forward work to develop closed head notes for closed judgments to summarise the broad subject of the judgment and to include key words for search purposes, in order to assist Special Advocates in accessing relevant case law.

---

<sup>1</sup> (2009) 49 EHRR 29

### Ability of Special Advocates to call expert witnesses

4. Special Advocates have raised concerns about their ability to call witnesses to challenge the Agencies on sensitive material. Special Advocates are now open to call experts and adduce evidence.<sup>2</sup> However, it would not be appropriate for serving or former employees of the Agencies to take on such a role, and in any case, Special Advocates may not view Agency employees as impartial. If the Special Advocate identifies another suitable witness, either the witness would have to be subject to rigorous security vetting or the questions would need to be posed in an open hearing following notification being given to the Secretary of State. We recognise that in some cases these options may not be practicable, and that is why we are recommending providing further training to Special Advocates (as outlined in paragraph 2.24), to ensure that they are able to understand and challenge sensitive material themselves. In addition, the Agencies are keen to help Special Advocates with specific or general enquiries where possible.

### Late service of material in proceedings

5. Special Advocates have raised concerns that the closed material is often provided to them very late, hindering their ability to function effectively. The Government always seeks to ensure that service of closed material is achieved according to the directions set by the court wherever possible and we reject the allegation that there is a systemic problem of late service of closed material by the Secretary of State. It is the courts who are responsible for setting the timetable for service of material and it is open to the judge to adjourn the proceedings if any real prejudice has been caused to the individual represented by the Special Advocate.

2 The Government changed the rules governing control order and asset freezing proceedings in 2009 to make clear that Special Advocates can call expert witnesses and adduce evidence. While it was already open to the Special Advocates to do so, this brought this element of the rules formally in line with those for the Proscribed Organisations Appeal Commission and the Special Immigration Appeals Commission, which were changed in 2007.

## Appendix G

### Remit of the Commissioners

#### Interception of Communications Commissioner

1. The main functions of the Interception of Communications Commissioner, appointed under section 57 of the Regulation of Investigatory Powers Act 2000 (RIPA), are to keep under review:

- ♦ the Secretary of State's role in authorising warranted interception
- \* the operation of the regime for the acquisition of communications data by public authorities
- \* the Secretary of State's role, in relation to intercepted material or communications data, in authorising the giving of notices imposing disclosure requirements in respect of encrypted information
- ♦ the adequacy of the arrangements in force for restricting the use of intercepted material and protecting encryption keys for intercepted material and communications data.

#### Intelligence Services Commissioner

2. The main functions of the Intelligence Services Commissioner, appointed under section 59 of RIPA, are to keep under review:

- \* the exercise of the Secretary of State's powers to issue, renew and cancel warrants for entry on or interference with property or with wireless telegraphy
- \* the exercise of the Secretary of State's powers to authorise acts done outside the UK, which may be unlawful without such an authorisation
- ♦ the exercise and performance of the Secretary of State's powers and duties in granting authorisations for intrusive surveillance and the investigation of electronic data protected by encryption
- ♦ the exercise and performance by members of the intelligence services of their powers and duties under Parts II and III of RIPA, in particular with regard to the grant of authorisations for directed surveillance, and for the conduct and use of covert human intelligence sources and the investigation of electronic data protected by encryption.



## Appendix H

# The Intelligence and Security Committee

1. The Intelligence and Security Committee (ISC) examines the expenditure, administration and policy of the Security Service, the Secret Intelligence Service and the Government Communications Headquarters (GCHQ). It has nine members drawn from both Houses of Parliament.

2. Members are appointed by the Prime Minister in consultation with the Leader of the Opposition. The ISC makes an annual report to the Prime Minister on the discharge of its functions. The Prime Minister lays this report before Parliament.

3. If it appears to the Prime Minister that the publication of any matter in a report would be prejudicial to the continued discharge of the functions of the security and intelligence agencies, the Prime Minister may exclude that

matter from the copy of the report laid before Parliament. Heads of Agencies may decline to disclose information to the ISC on the basis that it is sensitive information. The relevant Secretary of State has the power to overrule this decision if they decide it is in the public interest.

4. The appropriate Secretary of State also has a separate power to determine that information should not be disclosed to the ISC. This power cannot be exercised on national security grounds alone, and subject to that, the Secretary of State shall not make a determination not to disclose unless the information appears to them to be of such a nature that, if they were requested to produce it before a Departmental Select Committee of the House of Commons, they would think it proper not to do so.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

## Appendix I

### Possible model for an Inspector-General

1. An Inspector-General (IG) could oversee the powers and policies of the security and intelligence agencies and retrospectively review their operational activity. An IG for the Agencies could replace the Intelligence Services Commissioner and part of the remit of the Interception of Communications Commissioner.

2. An IG could be responsible for oversight of all the Agencies' covert investigation techniques, including the use of authorisations under the Intelligence Services Act 1994, and use by the Agencies of powers under the Regulation of Investigatory Powers Act 2000 (RIPA) Part I Chapter I (interception) and Chapter II (communications data), Part II (surveillance and CHIS) and Part III (encrypted data). It could also be responsible for oversight of requirements arising out of new government policies or legislation or the development of new practices. The IG could also provide legal advice and guidance to the Agencies on the use of their covert investigative techniques.

3. An IG could review the policies and procedures of the Agencies that relate to operational activities, including ethical matters. Ethical matters could be referred from, and reviewed, in close co-operation with the Staff Counsellor.

4. An IG could have a retrospective review function that would include the ability to launch its own enquiries into past Agency operational activity. It could have a right to request intelligence, subject to Ministerial veto.

5. This would create two distinct oversight bodies: one focused on the Agencies, and one on all other public authorities with RIPA powers.

The risk of this approach is that oversight of interception would be split between two different bodies, possibly leading to different standards or approaches emerging. This would need to be managed and would not necessarily be straightforward.

6. The IG could have a statutory duty to consult the Prime Minister on its annual work programme. It could produce an annual report for the Prime Minister, and publish reports on the outcome of the retrospective enquiries into Agency operational activity and reviews into operational policies. The IG could have a duty to develop an effective public profile for its work.

7. An IG could be appointed by, and answerable to, the Prime Minister. The post could have some form of pre-appointment scrutiny by Parliament and/or could be advertised publicly. The role could be filled by a suitably experienced judge. If this was not a judicial appointment, the IG could be a senior civil servant but would need to be supported by a legal adviser with the appropriate legal and/or judicial experience. The IG could head up a team which would include a Secretariat and specialists with responsibility for aspects of the work of the IG (e.g. interception).

## Appendix J

### Use of sensitive information in judicial proceedings: international comparisons

1. In preparing this Green Paper, the Government has surveyed a range of international practice in order to understand how other governments address the challenge of handling sensitive material in judicial proceedings. We have developed the proposals following full and careful consideration of the experience and approaches of other governments – including those who are signatories to the European Convention on Human Rights (ECHR) and those who are not, and both common law and civil law systems – and seeking to learn from their experience.

#### Summary of international comparisons research

2. The use of sensitive material in court proceedings relating to national security is a live issue and the subject of public debate in many countries. We believe that the large volume of complex counter-terrorism-related litigation in the UK has created a particularly acute set of pressures on the Government and the court system, which is not necessarily the case everywhere. Nonetheless, since 2001, many countries, including the Netherlands, Australia and Canada, have passed legislation in order to enhance their ability to rely on and protect sensitive information in hearings relating to national security. Provisions akin to Public Interest Immunity (PII), allowing the court to balance the public interest in disclosure against the public interest in non-disclosure, are very widely used, but have been supplemented in many jurisdictions by more tailored approaches in the national security context.

3. Several jurisdictions make use of **closed material procedures (CMPs)**, either in an immigration context or with wider application in civil and criminal procedures. In Canada, legislation provides for the use of CMPs and Special Advocates in certain circumstances, such as where a security certificate has been issued under the Immigration and Refugee Protection Act 2001 (IRPA). In 2009, the Danish Parliament passed legislation providing for the Justice Minister to request use of CMPs and Special Advocates in national security deportations. The arrangements in both Canada and Denmark, designed to protect information and ensure procedural fairness where the government is defending an appeal against an immigration decision which was based on sensitive information, bear some similarities to the UK's Special Immigration Appeals Commission (SIAC).

4. The Netherlands and Australia make limited use of CMPs in different contexts. In Australia, under the National Security Information (Criminal and Civil Proceedings) Act 2004, the Attorney General may issue a non-disclosure certificate for the purposes of a proceeding to which the Act applies, where there may be a disclosure of national security information, and if the Attorney General considers that the disclosure is likely to prejudice national security. The certificate provides for a closed hearing to determine if the information may be disclosed and in what form. Under this Act, national security information refers to information that relates to national security, or the disclosure of which may affect national security, defined as Australia's defence, security, international relations or law enforcement interests. In the Netherlands,

the Intelligence and Security Services Act 2002 allows the government to refuse to disclose sensitive material if disclosure would damage national security. With the claimant's consent, the material may be shared with the judge, who balances the claimant's interest against the public interest in non-disclosure in deciding whether to admit it as evidence. If the judge assesses that the public interest in non-disclosure is stronger than the information may, with the claimant's consent, still be admitted as evidence and be disclosed only to the court.

5. In Canada, **Special Advocates** have been a feature of the legislative immigration framework since 2008, as part of the IRPA. IRPA provides for use of CMPs and Special Advocates when the Government has issued a national security certificate on a case, indicating that the immigration decision was taken using sensitive information. In terms of communication between the Special Advocate and the individual(s) they represent, there have been more such attempts in Canada than in the UK, although the number is not high. We judge that higher levels of communication probably arise out of both legislative provisions and case law, as well as the practical approach to case management that has developed in Canada.

6. The Government considered the operation of systems based on an **inquisitorial model** of justice, to assess whether such systems reduced the risk of disclosure of sensitive information more effectively than adversarial systems. Our goal was to establish whether enhancing the case management powers of judges in the early stage of a case would result in cases being streamlined consistently and consequently fewer issues being contested during later stages of proceedings. Based on our research, we do not believe that any of the predominantly inquisitorial jurisdictions we surveyed have had to handle the volume of national security litigation we have seen in the UK, in particular anything on the scale of the Guantanamo civil damages claims. As such, it is difficult to draw direct comparisons and conclusions as to whether the active involvement of judges in case management is a significant factor in reducing their resource burden. As we have noted elsewhere in this Green Paper, a greater role for judges would likely mean a reduced role

for Special Advocates, and moreover a judge may conclude, based on initial fact-finding work, that the scope needs to be broadened rather than narrowed. It is also noteworthy that civil law systems with a largely inquisitorial heritage do feature adversarial elements after the initial stages of the case have been completed, and the trend has been for this to increase in recent years in response to the ECHR. Our consideration of international practice in this area thus supports our conclusion that there would be no clear benefits, but instead significant costs, from introducing more active case management powers for judges.

7. Similarly, no country we surveyed had established a **specialist court** to hear cases in which sensitive information would be considered, or had actively promoted judicial specialisation. In the Netherlands, most terrorist criminal cases are heard before the Rotterdam District Court, but this is for practical reasons, because the National Public Prosecutor on Counter-Terrorism is based in Rotterdam. As discussed elsewhere, we judge that sensitive information may arise in a broad range of types of case – many will be related to action the Government has taken as part of its approach to counter-terrorism, but this is not exclusively the case and moreover may change over time in response to real-world developments. We have therefore proposed that the Government work with existing judicial case-allocation systems, which over time should allow cases using sensitive material to be allocated to a judge with experience in the particular requirements of handling such material, but also with an appropriate specialist legal background. Our survey of international practice did not provide a compelling case for going beyond this.

8. We noted a range of practice in terms of the use of specific provisions, in legislation or elsewhere, to guide the **handling of foreign-sourced material**. Some countries make explicit provision for how foreign-sourced material should be handled, for example the law may set out the steps the UK Government is expected to take with the other government in order to seek permission to disclose the document. In other cases, foreign-sourced material is treated as one type of sensitive material and treated implicitly within the same

framework. In practice, the practical operation of either system and its ability to safeguard sensitive material from disclosure will depend to a great extent on the approach taken by the courts.

9. The only exception to the exercise of judicial discretion in the disclosure not only of foreign-sourced material but of any sensitive material, would be where the Government has in place some form of 'executive veto' on disclosure. Of the countries we surveyed, we understand provisions akin to an executive veto to exist only in Canada and the US, although some role for judicial challenge remains. In the US there are various mechanisms for the protection of classified information, principally but not limited to state secrets privilege (SSP), under which the relevant US Government agency or department, with the Attorney General's approval, may assert that information may not be disclosed where there is a reasonable expectation of significant harm to national security. These measures combine to provide effective safeguards against disclosure of sensitive information. Assertions of SSP, and the legal consequences of such claims, have been challenged in the US courts, most recently in the case of *Binyam Mohamed et al. v Jeppesen Dataplan, Inc.* However, where the privilege is properly asserted, the courts have generally upheld the claim, deferring to Executive assessments of the risk to national security. In Canada the power has never been used, but the Attorney General may, in certain limited circumstances, personally issue a certificate under the Canada Evidence Act 1985 prohibiting disclosure following a court order that it should be released. This veto is not unconditional and is subject to limited review by a judge, under the Canada Evidence Act 1985.

## Conclusion

10. A wide range of international partners face the same fundamental challenge of protecting sensitive information while ensuring that the courts have the tools available to deliver high standards of justice. However, as set out elsewhere in this Green Paper, the UK faces a unique and unprecedented set of circumstances. We face a high threat from terrorism. The Joint Terrorism Assessment Centre (JTAC), whose role is to provide independent assessments of the threat to the UK from international terrorism, has assessed the threat as at least severe between 2006 and 2009, and no lower than substantial since 2006. This threat demands a comprehensive and sophisticated response. The cornerstone of this response will always be police-led work to prosecute terrorists, and the Government has prosecuted 241 individuals since September 2001<sup>1</sup> for terrorism offences. But prosecution is not always possible and other actions, which support and complement prosecution, are equally important. This includes the Agencies' vital work to gather information on threats by working with foreign intelligence services, as well as a limited number of non-prosecution tools that enable Ministers to disrupt suspected terrorist activity.

11. The wide scope of this counter-terrorist activity has given rise to a range of legal challenges – including statutory appeals against executive action, civil claims for damages, judicial reviews and requests for 'Norwich Pharmacal' relief – which we believe is unusual internationally and exceptional among ECHR signatory states. We estimate that sensitive information is central to 27 cases<sup>2</sup> (excluding a significant number of appeals against executive actions) currently before the UK courts, and in many of these cases judges do not have the tools at their disposal to discharge their responsibility to deliver justice based on a full consideration of the facts. In the case of 16 civil claims brought by former residents of Guantanamo Bay, the sensitivity of the centrally

1 Home Office statistical bulletin 20 June 2011, Operation of police powers under the Terrorism Act 2006 and subsequent legislation: Arrests, outcomes and stop and searches, Quarterly update to December 2010

2 According to current records of the Treasury Solicitor's Department

relevant documents meant that the Government did not feel the court process would be able to deliver a judgment based on all the facts, and had little choice but to propose a mediated settlement in late 2010, with all the attendant disadvantages for the public purse and for the administration of justice.

12. In developing the proposals in this Green Paper we have given full and careful consideration to the approaches used by other countries. We have also been mindful of the specific circumstances we face in the UK, and the need to put forward proposals that are tailored to these circumstances and that will respond to the opportunity we now have to put the judicial system on a stronger long-term footing in meeting the needs of both justice and national security. The proposals build on other countries' experience where possible, and where necessary they propose more fundamental and far-reaching reform than has been attempted elsewhere – for example legislation to provide for the extension of CMPs to the range of civil proceedings. We believe that this is a proportionate and balanced response to the challenges we face, and that it will allow us to deliver standards of procedural fairness consistent with both our values as a nation and our international legal obligations.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

## Appendix K

### Equality duties and impact assessments

#### Equality

Under the Equality Act 2010, when exercising its functions, the Government has an ongoing legal duty to pay 'due regard' to:

- » the need to eliminate unlawful discrimination, harassment and victimisation
- » advancing equality of opportunity between different groups
- » fostering good relations between different groups.

The payment of 'due regard' needs to be considered against the nine 'protected characteristics' – namely race, sex, disability, sexual orientation, religion and belief, age, marriage and civil partnership, gender identity, and pregnancy and maternity.

The Government has a legal duty to investigate how policy proposals are likely to impact on the protected characteristics and take proportionate steps to mitigate the most negative ones and promote the positive ones.

Many of the most recent cases that illustrate the challenges of using sensitive information in civil proceedings have been taken by men from the following racial groups: Asian (British and South East), Arab (Middle Eastern) and North African; and the following religion: Islam.

At this stage, while this demonstrates a differential impact, the Government does not believe that there will be an adverse impact on any individual from any of these groups. The proposals on CMPs made in the Paper seek to improve fairness by

ensuring that all relevant information can be taken into account by the courts and will be available across the civil justice system generally. No firm proposals have been made in respect of inquests, but it is clear that changes could have a significant impact in Northern Ireland, affecting inquests into the deaths of a broad range of individuals from across the community, including members of the security forces, civilians and paramilitaries.

Given that the conclusions above are based on a small sample of cases and that the proposals have a potentially very broad application, it is unclear at this stage whether the patterns of impact identified above will continue. During the consultation period the Government will consult widely on the proposals, including with representative groups, and seek further views and evidence of the impact of the proposals on the protected characteristics.

**Please provide details of any evidence you are aware of which indicates that any of the proposals outlined will have either a positive or negative impact on any of the protected characteristics.**

### Impact assessments

The Government has carried out separate impact assessments in support of this Green Paper.

The impact assessments present the evidence base supporting the rationale for government intervention and estimate the costs, benefits, risks and wider impacts associated with the proposed options. They follow the procedures set out in the *Impact Assessment Guidance* and are consistent with the HM Treasury *Green Book*.

**In addition to responding to the consultation questions within the Green Paper, readers are also invited to comment on the analysis contained within the impact assessments.**

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION



# Glossary

Below is a list of key terms found in this Paper and how they are used in this particular context.

Term	Summary
<b>Active case management</b>	<p>A civil court in England and Wales is required under Rule 1.4 of the Civil Procedure Rules to further its overriding objective of hearing cases justly by actively managing cases. Active case management is defined in Rule 1.4(2) as including, but is not limited to, early identification of the issues, deciding the order in which issues are to be resolved, fixing timetables and controlling progress of the case. For the purposes of managing a case, the court has a wide range of general case management powers, listed in Rule 3, but those powers are not exclusive and are in addition to any other powers that the court may otherwise have. In the context of this consultation document, references to more active case management powers for judges mean giving the court such other, greater powers to determine the issues in the case and the relevance of certain evidence, which might, for example, include the power for the judge to cross-examine witnesses or order expert reports.</p>

Term	Summary
<p><b>Civil proceedings</b></p>	<p>For the purposes of this Green Paper any court or tribunal proceedings which are not criminal in nature are referred to as civil proceedings. Civil proceedings include, but are not limited to, areas such as public law (i.e. judicial review), negligence, family law, employment law, property law and commercial law.</p> <p>By contrast, criminal proceedings involve an accusation by the state (or in England, Wales and Northern Ireland, occasionally by way of a private prosecution) that the accused has committed a breach of the criminal law which, if proved, would lead to conviction and the imposition of a sentence. Crimes are generally wrongs which affect the public as a whole, so that the public has an interest in their detection and punishment.</p> <p>The proposals outlined in this Paper do not affect criminal proceedings.</p>
<p><b>Confidentiality ring</b></p>	<p>A confidentiality ring is an arrangement in England and Wales which may be agreed between the parties to civil litigation or ordered by the court whereby documents are disclosed only to a party's legal representatives but not to the parties to the litigation themselves. A confidentiality ring may be used in intellectual property or commercial cases where open disclosure would render the proceedings futile. A failure to abide by the agreement may amount to contempt of court.</p>
<p><b>Control order</b></p>	<p>The Prevention of Terrorism Act 2005 provides the Home Secretary with the power to impose a control order on an individual whom they reasonably suspect is or has been involved in terrorism-related activity and where they consider it is necessary for purposes connected with protecting members of the public from a risk of terrorism. A control order may impose any obligation on the individual that is necessary to prevent or restrict that individual's involvement in terrorism-related activity. Under the Terrorism Prevention and Investigation Measures (TPIM) Bill currently before Parliament, control orders are to be replaced by TPIM notices.</p>

Term		Summary
CPR	Civil Procedure Rules	<p>Consolidated rules of court governing (since 1999) the practice and procedure in civil proceedings in the Court of Appeal, High Court and County Courts in England and Wales.</p> <p>The courts in Scotland and Northern Ireland operate under their respective rules of court.</p>
Disclosure		The act of providing documents or information (sensitive or otherwise), whether under the relevant procedural rules or following a court order.
ECHR	European Convention on Human Rights	<p>An international agreement drafted after World War II by the Council of Europe (a separate body from the European Union). The UK ratified the Convention in March 1951, and it came into force in September 1953. The Convention is made up of a series of articles, each of which is a short statement defining a right or freedom, together with any permitted exceptions. The rights in the Convention apply to everyone within the jurisdiction of the states that are parties to the Convention.</p>
ECtHR	European Court of Human Rights	<p>A court established by the ECHR to hear cases where individuals or states assert that a state party to the ECHR has violated rights under the Convention. The Court is based in Strasbourg, France. States party to the ECHR are bound by the Court's judgments.</p>
Gisting		<p>A feature of closed material procedures: a summary of closed material is provided to the individual whenever it is possible to summarise that material without disclosing information contrary to the public interest. The AF (No.3) disclosure requirement (also sometimes referred to as 'gisting') goes further than this and requires Government to give the individual sufficient information about the allegations against them to enable them to give effective instructions to the Special Advocate, even if disclosure of that information is damaging to the public interest.</p>

Term		Summary
IAE	Intercept as evidence	The use of intercept material (e.g. telephone calls, emails and other internet communications) as evidence in criminal proceedings. Though this is not currently available, the Government is committed to seeking a practical way of allowing the use of intercept as evidence in court.
IPT	Investigatory Powers Tribunal	An independent tribunal through which individuals can raise allegations against the security and intelligence agencies of misuse of the powers set out in the Regulation of Investigatory Powers Act 2000 and complain about any other conduct by the security and intelligence agencies.
Judicial review		The procedure by which the decisions of a public body can be reviewed by the courts.
Ministerial responsibility		The ultimate responsibility for the actions of the security and intelligence agencies lies with their Secretaries of State: the Foreign Secretary for the Government Communications Headquarters and the Secret Intelligence Service, and the Home Secretary for the Security Service.
Natural justice		A term used to describe the need for fairness or 'due process' when a court or tribunal is determining the rights and obligations of parties.
Neither confirm nor deny		The policy of successive governments and of the security and intelligence agencies to neither confirm nor deny the veracity of claims or speculation about sensitive national security matters and to avoid comment on such matters generally.
Open court		The general rule is that a court hearing is to be in public, or 'open court', and may be attended by members of the public and the media (in England and Wales, see Civil Procedure Rules, Rule 39.2). In addition, judgments are made public and the media are permitted to report any open aspect of the proceedings
Private hearings		A private (or <i>in camera</i> ) hearing is part or all of a civil hearing from which the press and public are excluded but not the litigants and their legal advisers. (In England and Wales the circumstances in which a private hearing may be held are set out in the Civil Procedure Rules, Rule 39.2.)

Term	Summary
Public interest	<p>'Public interest' is not defined in legislation. It signifies something that is <b>in the interests of</b> the public as distinct from matters which are <b>of interest to</b> the general public. There are different aspects of the public interest, such as the public interest that justice should be done and should be seen to be done in: defence; national security; international relations; the detection and prevention of crime; and the maintenance of the confidentiality of police informers' identities, for example.</p>
Rule 43 Report	<p>A report written by a coroner pursuant to Rule 43 of the Coroners Rules 1984. The report is made to persons or organisations following the coroner's investigation, where the coroner feels that actions could potentially be taken by those persons or organisations to avoid future deaths, by using the lessons identified from the facts heard at the inquest. In Northern Ireland, a similar power exists in Rule 23(2) of The Coroners (Practice and Procedure) Rules (Northern Ireland) 1963.</p>
Special Advocate Support Office	<p>The office which provides support and instructions to Special Advocates in England and Wales.</p>
Sensitive material/information	<p>Any material/information which if publicly disclosed is likely to result in harm to the public interest. All secret intelligence and secret information is necessarily 'sensitive', but other categories of material may, in certain circumstances and when containing certain detail, also be sensitive. Diplomatic correspondence and National Security Council papers are examples of other categories of material that may also be sensitive.</p>

Term	Summary	
SIAC	Special Immigration Appeals Commission	The Special Immigration Appeals Commission was created by the Special Immigration Appeals Commission Act 1997. It deals with appeals in cases where the Home Secretary exercises their statutory powers to deprive an individual of their British citizenship, deport an individual from the UK, or revoke an individual's immigration status (which allows for an individual's exclusion from the UK) where there is reliance on information the disclosure of which would be contrary to the public interest on the grounds of national security, in the interests of the relationship between the UK and another country or for other public interest reasons.
Strike out		A court may strike out a claim if it decides that the claim has no reasonable prospect of success, or is an abuse of process, or would be against the public interest to proceed, and that it cannot be allowed to continue. In Scotland such a claim would simply be 'dismissed'.

PROCESSED BY CBIS UNDER THE  
PROVISIONS OF THE PERCY ACT AND/OR  
ACCESS TO INFORMATION ACT.  
REVISE PAR LE CBIS EN VERTU DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.



Information & publishing solutions

Published by TSO (The Stationery Office) and available from:

**Online**

[www.tsoshop.co.uk](http://www.tsoshop.co.uk)

**Mail, telephone, fax and email**

TSO

PO Box 29, Norwich NR3 1GN

Telephone orders/general enquiries: 0870 600 5522

Order through the Parliamentary Hotline Lo-Call: 0845 7 023474

Fax orders: 0870 600 5533

Email: [customerservices@tso.co.uk](mailto:customerservices@tso.co.uk)

Textphone: 0870 240 3701

**The Parliamentary Bookshop**

12 Bridge Street, Parliament Square,

London SW1A 2JX

Telephone orders/general enquiries: 020 7219 3890

Fax orders: 020 7219 3866

Email: [bookshop@parliament.uk](mailto:bookshop@parliament.uk)

Internet: [www.bookshop.parliament.uk](http://www.bookshop.parliament.uk)

**TSO@Blackwell and other accredited agents**

ISBN 978-0-10-181942-8



9 780101 819428

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

**TOP SECRET/COMINT  
(with attachment)  
For Information**

MAR - 3 2011

**MEMORANDUM TO THE MINISTER**

**2011 Threat Assessment**

I attach for your information a copy of the Service's 2011 Threat Assessment which reviews the events of 2010 and attempts to look forward to describe threat levels for this calendar year.

I would appreciate an opportunity to brief you on the Assessment.

A handwritten signature in black ink, appearing to read "R. Fadden", is positioned above the name of the signatory.

Richard B. Fadden.

Encl.

c.c. National Security Advisor  
Deputy Minister of Public Safety.

THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO MANDATORY EXEMPTION UNDER THE ACCESS TO INFORMATION ACT OR THE PRIVACY ACT. THE INFORMATION OR INTELLIGENCE MAY ALSO BE PROTECTED BY THE PROVISIONS OF SECTION 37(1) and 38(1) OF THE CANADA EVIDENCE ACT. THE INFORMATION OR INTELLIGENCE MUST NOT BE DISCLOSED OR USED AS EVIDENCE WITHOUT PRIOR CONSULTATION WITH THE CANADIAN SECURITY INTELLIGENCE SERVICE.





CENTRE INTÉGRÉ D'ÉVALUATION DES MENACES

INTEGRATED THREAT ASSESSMENT CENTRE

## ÉVALUATION DE LA MENACE

10 / 145-F

2010 11 30

Le présent document est coté SECRET. Il est la propriété du Centre intégré d'évaluation des menaces (CIEM) et a été préparé par lui. Il provient de diverses sources et contient des informations valables à la date de publication. Il est fourni à votre organisme ou ministère à titre confidentiel et peut être communiqué par votre organisme ou ministère aux personnes qui ont les cotes de sécurité nécessaires et les systèmes de sécurité appropriés pour conserver l'information. Il ne doit être ni reclassifié ni réutilisé, de quelque manière que ce soit, en tout ou en partie, sans le consentement de l'expéditeur. Tout commentaire doit être envoyé par courriel à CSIS-ITAC.

Pour communiquer avec le CIEM, veuillez passer par le Centre des opérations globale au

### RADICALISATION ISLAMISTE DANS LES PRISONS CANADIENNES

#### Faits saillants

- Dans plusieurs prisons canadiennes, des détenus dirigent les prières musulmanes.

cont'd...

- Les gangs de prison musulmans commencent à voir le jour dans les établissements correctionnels fédéraux du Canada.

## Introduction

1. Le présent document traite de la diffusion de la radicalisation et de l'islam radical dans les prisons canadiennes ainsi que de menace éventuelle que ces activités représentent pour la sécurité nationale. Il s'agit d'une mise à jour de l'évaluation de la menace du CIEM et n° 07/05A rédigée en 2007 et intitulée *Menace que font peser les conversions à l'islam radical dans les prisons canadiennes*. La période d'évaluation du présent document s'étend de mars 2006 à octobre 2010. Les informations proviennent de sources classifiées et non classifiées.

2. Le CIEM définit la radicalisation comme le fait de passer d'idées modérées à des croyances extrémistes. La radicalisation musulmane consiste à passer des croyances musulmanes modérées et courantes à la conviction que la violence peut être légitimement utilisée pour défendre une idée fondamentale de l'islam.

## Contexte

3. Au Canada, les gouvernements fédéral, provinciaux et territoriaux sont responsables de l'administration des services correctionnels, qui incluent la surveillance des délinquants en milieu carcéral et communautaire. Les autorités placent les délinquants adultes dans le système correctionnel correspondant en attendant les décisions des tribunaux.

4. Dans la plupart des cas, les délinquants accusés d'acte criminel sont détenus dans des prisons ou des centres de détention provinciaux ou territoriaux pendant les procès. Pour sa part, le Service correctionnel du Canada (SCC) est responsable des délinquants purgeant une peine de deux ans ou plus qui nécessitent un transfert entre des établissements correctionnels. Les

délinquants dont la liberté conditionnelle a été suspendue sont temporairement détenus dans des établissements provinciaux ou territoriaux jusqu'à un examen du dossier. Ainsi, les détenus condamnés par un tribunal fédéral purgent leur peine dans des établissements provinciaux ou territoriaux, ainsi que fédéraux.

#### *Service correctionnel fédéral*

5. Le SCC supervise 57 établissements de différents niveaux de sécurité allant de minimal à maximal, en plus de 16 centres correctionnels communautaires, 84 bureaux de libération conditionnelle et quatre pavillons de ressourcement. Il entretient également des partenariats avec des organisations non gouvernementales qui gèrent plus de 200 établissements résidentiels communautaires partout au Canada.

6. En date du 8 octobre 2010, le SCC s'occupe de 22 358 délinquants purgeant une peine de deux ans ou plus, dont 13 768 détenus et 8 590 en liberté conditionnelle et en liberté surveillée dans la communauté. De ces détenus, 711 sont des musulmans incarcérés dans des pénitenciers fédéraux, notamment en Ontario (288) et au Québec (220). Le nombre de détenus musulmans représente 5,2 % de la population carcérale nationale dans les pénitenciers fédéraux. Cependant, puisque 533 détenus, ou 2,4 % de cette population, n'ont pas indiqué leur appartenance religieuse, le pourcentage réel de détenus musulmans pourrait être légèrement supérieur.

7. De 2002 à octobre 2010, le nombre de détenus musulmans a augmenté de 86 %. Dans la même période, la population carcérale a augmenté de 8,4 %. Ces statistiques ne prennent pas en compte les conversions religieuses au cours de la détention, car la plupart du temps, les autorités correctionnelles ne notent les informations liées à l'appartenance religieuse d'un détenu que lors de l'évaluation initiale.

#### *Services correctionnels provinciaux et territoriaux*

8. Les ministères provinciaux et territoriaux gèrent 122 établissements correctionnels partout au Canada. On retrouve dans ces établissements des détenus en détention provisoire, des délinquants qui attendent d'être expulsés et des criminels qui purgent une peine de moins de deux ans.

9. La gestion des données de fonctionnement varie entre les différents services correctionnels provinciaux et territoriaux.

Selon un rapport datant de

2009 de Statistique Canada, quelle que soit la période, il y a environ 23 750 personnes incarcérées au Canada. Il est donc possible de déduire qu'il y a environ 10 000 détenus dans les établissements correctionnels provinciaux et territoriaux.



### Apparition de gangs musulmans dans les prisons

32. Les autorités correctionnelles fédérales ont noté la création de gangs musulmans dans leurs établissements.

PROCESSED BY CSIS UNDER THE  
PROVISIONS OF THE PRIVACY ACT AND/OR  
ACCESS TO INFORMATION ACT  
REVISÉ PAR LE SCRS EN VERTUE DE LA LOI  
SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS  
À L'INFORMATION.

Le présent document peut faire l'objet d'une exception aux termes de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*. On pourra également s'opposer à la communication des informations ou des renseignements qu'il contient en vertu de la *Loi sur la preuve au Canada*. Ces informations ou renseignements ne doivent être ni communiqués ni utilisés comme preuve sans consultation préalable du Service canadien du renseignement de sécurité. Comme la divulgation du présent document pourrait être préjudiciable à la sécurité nationale, le Service canadien du renseignement de sécurité (SCRS) interdit donc qu'il soit divulgué devant un tribunal, une personne ou quiconque ayant le pouvoir d'en ordonner la production ou la divulgation. Le SCRS prendra toutes les mesures prescrites par la *Loi sur la preuve au Canada* ou toute autre loi afin d'empêcher la production ou la divulgation de ces informations ou de ces renseignements, ce qui comprend toute attestation nécessaire faite au Procureur général du Canada.

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

SECRET  
(With attachment)

JAN 28 2011

**MEMORANDUM FOR THE MINISTER**

**RE: Islamic Extremist Radicalization in Canadian Prisons**

You may recall that a few months ago, I mentioned to you that we were preparing an assessment. I attach the above ITAC Threat Assessment which I thought you might find of interest.

I should note that the Assessment is giving added impetus for a closer relationship with

I would also like to acknowledge

On the substance of the Assessments,

A handwritten signature in black ink, appearing to read 'R. B. Fadden'.

Richard B. Fadden

Encl.

c.c. National Security Advisor  
Commissioner of Corrections  
Deputy Minister of Public Safety.