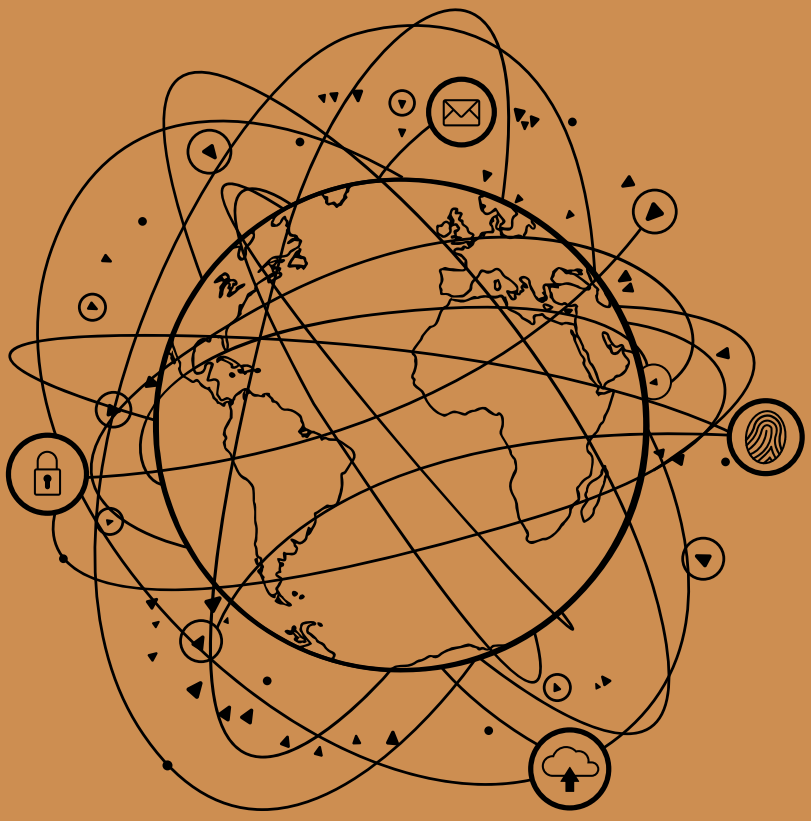
PRIVACY INTERNATIONAL

Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards



April 2018

This report is solely authored by Privacy International and does not represent the views of any of the other organisations mentioned within it.

Privacy International thanks Asaf Lubin and Thaya Uthayophas for their research assistance, which contributed to the preparation of this report.

Contents

I. Introduction	003
II. Background	005
A. What Do We Mean by Intelligence Sharing?	005
B. What Does Modern Intelligence Sharing Look Like?	005
C. What Do Intelligence Sharing Arrangements Look Like?	007
III. Human Rights Concerns	010
A. Intelligence Sharing and the Right to Privacy	011
B. Intelligence Sharing and Serious Human Rights Abuses	012
C. Intelligence Sharing and Accountability	014
IV. Legality and Intelligence Sharing	016
A. The Principle of Legality	016
B. Intelligence Sharing and the Principle of Legality	018
1. Secret Intelligence Sharing Arrangements	019
2. Lack of Domestic Legislation	023
V. Oversight and Intelligence Sharing	028
A. Oversight	028
B. Intelligence Sharing and Oversight	030
C. Trends and Concerns in the Oversight of Intelligence Sharing	032
1. Access to Intelligence Sharing Arrangements	032
2. Independent Oversight	034
a. Ex Ante Authorisation	035
b. Ex Post Monitoring	035
3. Collaboration Among Oversight Bodies	040
VI. Recommendations	042
Annex I – List of Oversight Bodies Contacted	049
Annex II – List of Partner Organisations	052
Annex III – Responses Received from Oversight Bodies	053
Annex IV – Selected Disclosure from Privacy International Five Eyes Litigation	129

I. Introduction

Intelligence sharing is one of the most pervasive, and least regulated, surveillance practices in our modern world. It is facilitated by rapidly changing technology that has allowed for the collection, storage and transfer of vast amounts of data within and between countries. The privacy impacts of these developments are significant. In this report, Privacy International offers a set of recommendations aimed at addressing the legality and oversight gaps of intelligence sharing arrangements.

In the past few decades, methods of communication have dramatically changed. The development of new technology, especially the birth of the internet, has transformed the way individuals communicate with each other and increased the amount of information that can be collected by several orders of magnitude. In particular, communications – emails, instant messages, calls, social media posts, web searches, requests to visit a website – may transit multiple countries before reaching their destination. The dispersion of communications across the internet vastly increases the opportunities for communications and data to be intercepted by foreign governments, who may then share them with other governments.

As methods of communications have dramatically changed, so too has intelligence gathering. Intelligence agencies have developed increasingly advanced ways of accessing, acquiring, storing, analysing and disseminating information. In particular, they have developed methods for acquiring communications and data traveling the internet. The costs of storing this information have decreased dramatically and continue to do so. At the same time, technology now permits revelatory analyses of types and amounts of data that were previously considered meaningless or incoherent. Finally, the internet has facilitated remote access to information, meaning the sharing of communications and data no longer requires physical transfer from sender to recipient.

The new scope and scale of intelligence gathering has given rise to a new scope and scale of the sharing of that intelligence between governments, particularly in response to threats to national security. Despite these dramatic changes, in many countries around the world, the public remains in the dark regarding state surveillance powers and capabilities, and whether those powers and capabilities are subject to the necessary safeguards pursuant to domestic and international law. One area of particular obscurity is arrangements between countries to share intelligence. These arrangements are typically confidential and not subject to public scrutiny.

As surveillance is conducted by different state actors, so is the sharing of such intelligence. The most opaque, and arguably the most extensive, sharing takes place between intelligence agencies, and this type of intelligence sharing is therefore the focus of this report. However, other state security actors as well as law enforcement

agencies also engage in information sharing. For example, the European Union is moving to link law enforcement and migration control databases and considering ways to allow member states to access these databases.[1] At the global level, the United Nations Security Council recently passed Resolution 2396, demanding that states undertake a range of measures to enhance intelligence sharing as a tool for combatting terrorism, including by collecting and sharing passenger name records ("PNRs") and developing and sharing lists or databases of known and suspected terrorists.[2]

Privacy International recognises the importance and benefit of intelligence sharing, for example, in the context of preventing acts of terrorism or identifying other serious threats to national security. Intelligence sharing does not violate international human rights law per se. But it does interfere with fundamental human rights, including the right to privacy. Thus, just as government surveillance must be transparent and subject to adequate safeguards and oversight, so too must intelligence sharing arrangements. Non-transparent, unfettered and unaccountable intelligence sharing, on the other hand, poses substantive risks to human rights and the democratic rule of law.

In September 2017, Privacy International – in partnership with 40 national civil society organisations – wrote to oversight bodies in 42 countries as part of a project to increase transparency around intelligence sharing and to encourage oversight bodies to scrutinise the law and practice of intelligence sharing in their respective countries.[3] Over the past few months, we have received responses from oversight bodies in 21 countries.[4]

This report is a follow-up to our outreach to oversight bodies in September 2017. Part II provides essential background, by explaining what we mean by intelligence sharing and what both modern intelligence sharing and intelligence sharing arrangements look like. Part III presents the human rights concerns presented by intelligence sharing. Part IV considers issues related to the legality of intelligence sharing. Part V considers issues related to the oversight of intelligence sharing. This Part also provides a summary of responses received from oversight bodies, focusing on the regulation of intelligence sharing in national laws and the practices of oversight bodies. The report concludes with a series of recommendations aimed at addressing the legality and oversight gaps of intelligence sharing practices.

1 See Council of the European Union, Council conclusions on improving criminal justice in cyberspace, 9 June 2016.

2 See UN Security Council, Resolution 2396, UN Doc. S/RES/2396, 21 Dec. 2017. This resolution builds upon prior UN Security Council calls to increase intelligence sharing in the counter-terrorism context. See, e.g., UN Security Council, Resolution 1373, UN Doc. S/RES/1373, 28 Sept. 2001.

3 For the full list of organisations and oversight bodies contacted, see Annexes I and II.

4 For all the responses received by Privacy International, see Annex III.

II. Background

A. What Do We Mean by Intelligence Sharing?

Intelligence sharing is one form of intelligence cooperation between states, which may also include operational cooperation, facilities and equipment hosting, training and capacity building, and technical and financial support.[5] Governments share intelligence in various ways. Pursuant to an intelligence sharing arrangement, a government might, inter alia:

- Access "raw" (i.e. unanalysed) information, such as internet traffic intercepted in bulk from fibre optic cables by another government;
- Access information stored in databases held by another government or jointly managed with another government;
- Receive the results of another government's analysis of information, for example, in the form of an intelligence report.

All forms of intelligence sharing raise concerns for privacy and other human rights. But the risks posed to these rights is particularly acute where a government can directly access information acquired or held by another government. Those risks are amplified by the increasing scope and scale of surveillance conducted by intelligence agencies, which has also given rise to a new scope and scale of sharing, discussed below.

B. What Does Modern Intelligence Sharing Look Like?

Over the last few years, the Edward Snowden disclosures and the resulting examination of intelligence practices have offered the public a rare glimpse into how surveillance has evolved in the digital age and, in turn, how that evolution has resulted in dramatic changes in the way intelligence can be shared between governments.

5 See Hans Born et al., Making International Intelligence Cooperation Accountable, 2015, pp. 18-21.

To begin, the Snowden disclosures revealed the wide scope of surveillance, primarily by the governments of the United States and the United Kingdom. Some of the earliest revelations concerned a US program called "Upstream", which taps the internet "backbone", the "network of high-capacity cables, switches, and routers that carry Americans' domestic and international internet communications."[6] The geographic location of the US features a high concentration of cables emanating from its east and west coasts. Moreover, the concentration of internet companies in California means that many of the world's communications – Gmail messages, Whatsapp texts, Facebook posts – may travel to servers in the US in the course of their transmission. The UK has a similar program tapping fibre-optic cables landing in the UK.[7] The UK's geographic location also makes it a natural landing hub for many of these cables.[8]

The US government also conducts sweeping mass surveillance programs beyond its borders. RAMPART-A, for example, is a National Security Agency ("NSA") program, operated in conjunction with foreign partners, that aims to gain "access to high capacity international fiber-optic cables that transit at major congestion points around the world."[9] A leaked NSA document indicates that RAMPART-A can intercept "over 3 Terabits per second of data streaming world-wide and encompasses all communication technologies such as voice, fax, telex, modem, e-mail internet chat, Virtual Private Network (VPN), Voice over IP (VoIP), and voice call records."[10] MUSCULAR was a program operated jointly with the UK's Government Communications Headquarters ("GCHQ"), which intercepted and extracted data directly as it transited to and from Google and Yahoo's private data centres, which are located around the world. According to a leaked 2013 document, in one 30-day period, the NSA sent over 181 million records – consisting of content and metadata – back to data warehouses at its headquarters in Fort Meade, Maryland.[11]

6 Ashley Gorski & Patrick C. Toomey, "Unprecedented and Unlawful: The NSA's 'Upstream' Surveillance", Just Security, 19 Sept. 2016, https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-surveillance/; see also Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2 July 2014; Charlie Savage, "N.S.A. Said to Search Content of Messages to and from U.S.", NY Times, 8 Aug. 2013, https://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html.

7 See Ewen MacAskill et al., "GCHQ taps fibre-optic cables for secret access to world's communications", The Guardian, 21 June 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

8 For a map of the world's submarine fibre-optic cables, see TeleGeography, Submarine Cable Map, https://www.submarinecablemap.com/.

9 For NSA slides providing an overview of RAMPART-A, see https://www.eff.org/files/2014/06/23/rampart-a_overview.pdf.

10 The document can be found at http://www.statewatch.org/news/2014/jun/usa-nsa-foreignpartneraccessbudgetfy2013-redacted.pdf.

11 See Barton Gellman & Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say", Wash. Post, 30 Oct. 2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

The Snowden documents further revealed the enormous scope and scale of sharing, particularly through foreign government access to information acquired under the various US mass surveillance programs. XKEYSCORE, for example, is an NSA "processing and query system", fed by "a constant flow of Internet traffic from fiber optic cables that make up the backbone of the world's communication network, among other sources."[12] As of 2008, XKEYSCORE "boasted approximately 150 field sites . . . consisting of over 700 servers", which store "'full-take data' at the collection sites—meaning that they captured all of the traffic collected." XKEYSCORE is accessible to certain foreign governments, including the Five Eyes – the US, UK, Australia, Canada and New Zealand – whose analysts can then "query the system to show the activities of people based on their location, nationality and websites visited."[13]

Marina, the NSA's metadata repository, is integrated into XKEYSCORE, meaning that it is also available to certain foreign governments, including the Five Eyes.[14] According to an introductory guide for NSA field agents disclosed by Snowden, Marina aggregates metadata intercepted from an array of sources, including bulk interception through the NSA's fibre-optic cable tapping programs. The guide explains that "[o]f the more distinguishing features, Marina has the ability to look back on the last 365 days' worth of . . . metadata seen by the [signals intelligence] collection system, **regardless** whether or not it was tasked for collection."[15] One of the Snowden disclosures revealed a GCHQ legal training slideshow, which suggests that gaining access to databases like Marina is relatively easy, requiring analysts to undergo "'multiple choice, open-book' tests done at the agent's own desk on its 'iLearn' system."[16]

C. What Do Intelligence Sharing Arrangements Look Like?

It is impossible to provide a complete map of intelligence sharing arrangements in place around the world. One of the best known sharing arrangements is the Five Eyes alliance between the US, UK, Australia, Canada and New Zealand. But despite being over 70 years old, little is known about the alliance, including the current agreement(s) that govern it.[17]

---

12 Morgan Marquis-Boire, Glenn Greewald & Micah Lee, "XKEYSCORE: NSA's Google for the World's Private Communications", The Intercept, 1 July 2015, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/. For NSA slides providing an overview of XKEYSCORE, see https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf.

13 Marquis Boire et al., "XKEYSCORE", supra.

14 See the NSA slides providing an overview of XKEYSCORE at https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf.

15 James Ball, "NSA stores metadata of millions of web users for up to a year, secret files show", The Guardian, 30 Sept. 2013, https://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents (emphasis in original).

16 Ewen MacAskill & James Ball, "Portrait of the NSA: no detail too small in quest for total surveillance", The Guardian, 2 Nov. 2013, https://www.theguardian.com/world/2013/nov/02/nsa-portrait-totalsurveillance.

17 For an overview of what we do know about the Five Eyes alliance, see Privacy International, Eyes Wide Open, 26 Nov. 2013, available at https://www.privacyinternational.org/report/1126/eyes-wide-open.

The NSA has developed a broader web of intelligence sharing partnerships. Among the Snowden disclosures was a 2013 NSA slide titled "Approved SIGINT Partners", which lists the countries with which the NSA exchanges signals intelligence.[18] The slide lists the Five Eyes countries as "Second Parties" and lists a further 33 countries as "Third Parties".[19] Even less is known about this latter web of arrangements, which also include many partnerships that incorporate the Five Eyes, such as:

- SIGINT Seniors Europe ("SSEUR", the Five Eyes plus Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain and Sweden)
- SIGINT Seniors Pacific ("SSPAC", the Five Eyes plus France, India, Singapore, South Korea, Thailand)[20]
- Nine Eyes (the Five Eyes plus Denmark, France, the Netherlands and Norway)
- 14-Eyes (the Nine Eyes plus Belgium, Germany, Italy, Spain and Sweden)
- 43-Eyes (the 14-Eyes plus the addition of the 2010 members of the International Security Assistance Forces to Afghanistan)[21]

18 This slide was first published in Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, 2014.

19 Third party partners occupy a "step below" second party partnerships and "the actual scope of the relationship can vary from country to country and from time to time." "NSA's Foreign Partnerships", Electrospaces.net, 4 Sept. 2014, https://electrospaces.blogspot.co.uk/2014/09/nsas-foreign-partnerships.html.

20 For recent reporting, including newly released Snowden disclosures, on SSEUR and SSPAC, see Ryan Gallagher, "The Powerful Global Spy Alliance You Never Knew Existed", The Intercept, 1 Mar. 2018, https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.

21 See "Five Eyes, 9-Eyes, and Many More", Electrospaces.net, 15 Nov. 2013, http://electrospaces.blogspot.co.uk/2013/11/five-eyes-9-eyes-and-many-more.html. The full list of 43 Eyes states are as follows: US, UK, Australia, Canada, New Zealand, Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Macedonia, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, and Ukraine. Privacy International acknowledges that the make-up of this alliance may have shifted over time. The general lack of clarity around intelligence sharing arrangements makes it difficult to confirm their exact scope.



Similarly, little is known about the bilateral and multilateral intelligence sharing arrangements spanning other geographic regions. Examples include:

- The Club de Berne is an intelligence sharing arrangement between the intelligence services of the members of the EU.

- The Shanghai Cooperation Organization is a security, economic and political cooperation forum in which intelligence sharing is undertaken between China, India, Kazakhstan, Kyrgyzstan, Pakistan, Russia, Tajikistan, and Uzbekistan.[22]

- Russia, Iraq, Iran and Syria have formed an intelligence sharing arrangement to facilitate cooperation in combating the Islamic State.[23]

22 Eleanor Albert, "The Shanghai Cooperation Organization Backgrounder", Council on Foreign Relations, 14 Oct. 2015, https://www.cfr.org/backgrounder/shanghai-cooperation-organization.

23 J. Dana Stuster, "Russia, Iran, Iraq, and Syria to Share Intelligence on Islamic State", Foreign Policy, 28 Sept. 2015, http://foreignpolicy.com/2015/09/28/russia-iran-iraq-and-syria-to-share-intelligence-on-islamic-state/.

III. Human Rights Concerns

Intelligence sharing can have significant implications for human rights. Below, Privacy International emphasises three areas of concern:

A. Intelligence Sharing and the Right to Privacy

B. Intelligence Sharing and Serious Human Rights Abuses

C. Intelligence Sharing and Accountability

Intelligence Sharing and Human Rights: A Summary

- Intelligence sharing constitutes an interference with the right to privacy and must therefore be subject to relevant protections under international human rights law, including the principles of legality, proportionality and necessity. The secrecy surrounding intelligence sharing arrangements and the absence of legal frameworks governing them render many of these arrangements incompatible with international human rights law.
- Intelligence sharing may permit states access to data collected through mass surveillance programs. Today, intelligence sharing is not confined to the handover of discrete information, but can encompass direct and unfettered access to “raw” (i.e. unanalysed) data as it transits the internet or held in databases.
- Intelligence sharing may permit States to circumvent constraints on domestic surveillance by allowing them to rely on their partners to obtain and then share information. An example of a common constraint is domestic restrictions on the types of techniques a State may use to conduct surveillance.
- States may share intelligence that may be used to facilitate serious human rights abuses, including extrajudicial killings; unlawful arrest or detention; or torture and other cruel, inhuman or degrading treatment. In states with authoritarian governments, weak rule of law and/or a history of systematically violating human rights, certain groups may be particularly vulnerable to abuse, such as dissidents, journalists and human rights defenders.
- States may receive intelligence from states that was derived from violations of international law, including through torture and other cruel, inhuman or degrading treatment. Intelligence obtained in violation of international law may also raise concerns regarding its reliability.
- Intelligence sharing poses fundamental accountability challenges. Agencies are constrained in their ability to influence or verify how information will be used or to subsequently substantiate how it was used. They are similarly constrained in their ability to verify or substantiate the provenance and other details of information shared by another state. These limitations may incentivise agencies to skirt accountability both for outbound and inbound sharing. In addition, many intelligence sharing arrangements prohibit the disclosure of shared information with third parties, which may include oversight mechanisms.

A. Intelligence Sharing and the Right to Privacy

As a form of surveillance, intelligence sharing constitutes an interference with the right to privacy. There are a range of different ways that an intelligence agency may obtain communications and other personal data, from targeted interception to collection in bulk. That agency may then provide other intelligence agencies with access to the material obtained. Those other intelligence agencies may then extract, store, analyse and further share that material. But fundamentally speaking, whether an intelligence agency initially obtains communications and data, or accesses communications and data obtained by another intelligence agency, the nature of the interference with the right to privacy is the same.

Because intelligence sharing constitutes an interference with the right to privacy, international human rights law must apply to this practice. For that reason, the UN Human Rights Committee has repeatedly stated, in reviewing the intelligence sharing practices of certain states parties to the International Covenant on Civil and Political Rights ("ICCPR"), that laws and polices regulating such sharing must be in full conformity with obligations under the ICCPR. The Committee has noted in particular the need to adhere to Article 17, which protects the right to privacy, "including the principles of legality, proportionality and necessity".[24]

Intelligence sharing also poses the risk that states may use it to circumvent constraints on domestic surveillance by allowing them to rely on their partners to obtain and then share information.[25] This risk is all the more heightened by the current lack of transparency, accountability and oversight of intelligence sharing arrangements. Examples of common constraints on domestic surveillance include restrictions on the types of techniques a state may use to conduct surveillance or on a state's ability to conduct surveillance on its own citizens or residents or members of a protected profession, such as journalists, lawyers and members of parliament.

24 UN Human Rights Committee, Concluding Observations on the Seventh Periodic Report of Sweden, UN Doc. CCPR/C/SWE/CO/7, 28 Apr. 2016, paras. 36-37; see also UN Human Rights Committee, Concluding Observations on the Initial Report of Pakistan, UN Doc. CCPR/C/PAK/CO/1, 23 Aug. 2017, para. 35; UN Human Rights Committee, Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, UN Doc. CCPR/C/GBR/ CO/7, 17 Aug. 2015, para. 24; UN Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Canada, UN Doc. CCPR/C/CAN/CO/6, 13 Aug. 2015, para. 10.

25 See Born et al., Making International Intelligence Cooperation Accountable, supra, at pp. 48-50; European Commission for Democracy through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006, 7 Apr. 2015, para. 11; Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection, 5 June 2015, p. 11 (noting that "the principle of making data available to other authorities should not be used to circumvent European and national constitutional data-protection standards"); Craig Forcese, "The Collateral Casualties of Collaboration: The Consequences for Civil and Human Rights of Transnational Intelligence Sharing", in International Intelligence Cooperation and Accountability, Pre-Conference Draft Paper, Conference on Intelligence Sharing, sponsored by the Norwegian Parliamentary Intelligence Oversight Committee, 5 Mar. 2009, pp. 90-92, available at https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=1354022.

It is not clear, for instance, how these constraints might meaningfully apply where a state accesses or receives data obtained in bulk by another state. States may also explicitly use intelligence sharing arrangements to obtain information they could not otherwise obtain through surveillance carried out by its own agencies.

The UN High Commissioner for Human Rights has accordingly observed:

> "There is credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections providedby domestic legal regimes. Such practice arguably fails the test of lawfulness because, as some contributions for the present report pointed out, it makes the operation of the surveillance regime unforeseeable for those affected by it. It may undermine the essence of the right protected by article 17 of the International Covenant on Civil and Political Rights, and would therefore be prohibited by article 5 thereof."[26]

B. Intelligence Sharing and Serious Human Rights Abuses

States may share intelligence with other states, who may then use that intelligence in a manner that facilitates serious human rights abuses. In some instances, states may knowingly share information with states that have a record of violating international law, including international human rights and international humanitarian law. In other instances, states may not necessarily anticipate that the intelligence they share will be used by other states to facilitate serious human rights abuses. However, in either set of circumstances, states that share intelligence that recipient states then use to facilitate such abuses may also bear responsibility for those abuses.[27]

26 UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, 30 June 2014, para. 30.

27 See Born et al., Making International Intelligence Cooperation Accountable, supra, at p. 42; International Commission of Jurists Eminent Jurists Panel, Assessing Damage, Urging Action, 2009, p. 90.

The UN Special Rapporteur for Counter-Terrorism has described the problem as follows:

> "Information sent to a foreign government or intelligence service may contribute to legal limitations on the rights of an individual but could also serve as the basis for human rights violations. . . . It is good practice to maintain an absolute prohibition on the sharing of any information if there is a reasonable belief that sharing information could lead to the violation of the rights of the individual(s) concerned. In some circumstances, State responsibility may be triggered through the sharing of intelligence that contributes to the commission of grave human rights violations."[28]

Intelligence shared by one state with another can contribute to a variety of serious human rights abuses. This risk is particularly acute where intelligence is shared with states with authoritarian governments, weak rule of law and/or a history of systematically violating human rights. In these contexts, such intelligence may form the basis for extrajudicial killings or contribute to unlawful arrest or detention or to torture and other cruel, inhuman or degrading treatment.[29] Moreover, certain groups may be particularly vulnerable to these abuses, such as dissidents, journalists and human rights defenders.[30]

In addition, intelligence received by one state from another may have been obtained in violation of international law, including through torture and other cruel, inhuman or degrading treatment. As the UN Special Rapporteur for Counter-Terrorism has stated: "Both the sending and receipt of intelligence can have important implications for human rights and fundamental freedoms. . . . [I]ntelligence received from a foreign entity may have been obtained in violation of international human rights law."[31] Furthermore, intelligence obtained in violation of international law may raise concerns regarding its reliability.

28 Martin Scheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, UN Doc. A/HRC/14/46, 5 May 2010, para. 41.

29 See Born et al., Making International Intelligence Cooperation Accountable, supra, at pp. 43-45; International Commission of Jurists, Assessing Damage, supra, at pp. 81-85.

30 See Born et al., Making International Intelligence Cooperation Accountable, supra, at pp. 40-41, 45.

31 Report of the Special Rapporteur on counter-terrorism, Compilation of good practices, supra, at para. 47.

C. Intelligence Sharing and Accountability

Intelligence sharing inherently poses a number of accountability challenges. Generally speaking, intelligence agencies lack control over the actions of their foreign partners. Moreover, they cede control over information once shared, despite whatever limitations ("caveats") may be attached to the sharing of that information. Their ability to influence or verify how that information will be used or to subsequently substantiate how it was used will be subject to significant limitations. Their ability to verify or substantiate the provenance and other details regarding information shared by another state will be similarly constrained.[32]

These inherent limitations can further facilitate the shirking of accountability over intelligence sharing. Because it can be so difficult to influence, verify or substantiate the use of information – or the means by which information was obtained – it can be easy for states sharing intelligence to assert "plausible deniability". Indeed, intelligence agencies have strong incentives not to make robust inquiries, for fear of damaging partnerships with foreign agencies.[33] And national oversight mechanisms typically have remit only over the activities of their national intelligence agencies.[34]

In addition to inherent limitations on accountability over intelligence sharing, there are common constraints imposed by states themselves. In particular, many intelligence sharing arrangements prohibit the disclosure of information shared between agencies to third parties, which may include oversight mechanisms, without the prior consent of the state from which the information originated. This prohibition is typically referred to as the "third party rule" or the "originator control principle". A requirement that oversight bodies seek the consent of a foreign intelligence agency to access information is fundamentally detrimental to oversight. As a matter of principle, requiring oversight bodies to seek such permission can cripple their independence. And as a matter of practice, foreign partners are unlikely to consent to such a request.[35]

32 See Born et al., Making International Intelligence Cooperation Accountable, supra, at pp. 38-39.

33 See European Commission for Democracy through Law (Venice Commission), Report on the Democratic Oversight of the Security Services, Study No. 388/2006 CDL-AD(2007)016, 11 June 2007, paras. 120-21.

34 See Hans Born & Aidan Wills, Overseeing Intelligence Services: A Toolkit, 2012, p.132.

35 See Born et al., Making International Intelligence Cooperation Accountable, supra, at p. 152.

The Council of Europe Commissioner for Human Rights has expressed concerns regarding the third party rule:

> "Given the amount of information that is received from foreign bodies, it is essential that oversight bodies' access is not limited to information generated by the security services they oversee – meaning that they cannot view information of foreign provenance. Given that services collaborate more than ever with foreign partners and hold in their files an increasing amount of information supplied by foreign services, this would have the effect of shielding operations or areas of activity from independent scrutiny."

The Commissioner has accordingly recommended that states parties:

> "ensure that access to information by oversight bodies is not restricted by or subject to the third party rule or the principle of originator control. This is essential for ensuring that democratic oversight is not subject to an effective veto by foreign bodies that have shared information with security services. Access to information by oversight bodies should extend to all relevant information held by security services including information provided by foreign bodies."[36]

36 Council of Europe Commissioner for Human Rights, Democratic and effective oversight of national security services, 2015, recommendation 16.

IV. Legality and Intelligence Sharing

A. The Principle of Legality

International human rights law provides that any interference with the right to privacy must be in accordance with the law.[37] At the heart of the principle of legality is the important premise that placing "intrusive surveillance regimes on a statutory footing" subjects them to "public and parliamentary debate".[38] Legality is also closely tied to the concept of "arbitrary interference", the idea being that the exercise of a secret power carries the inherent risk of its arbitrary application.[39]

The meaning of "law" implies certain minimum qualitative requirements of accessibility and foreseeability. The UN Human Rights Committee has elaborated on the meaning of "law" for the purposes of Article 19 of the International Covenant on Civil and Political Rights ("ICCPR"), which protects the right to freedom of opinion and expression, as follows:

37 See Article 17(1), International Covenant on Civil and Political Rights ("ICCPR") ("No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . . ."); Article 11, American Convention on Human Rights ("ACHR") ("2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence . . . . 3. Everyone has the right to the protection of the law against such interference . . . ."); Article 8(2), European Convention of Human Rights ("ECHR") ("There shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as is in accordance with the law . . . ."); see also UN Human Rights Committee, General Comment No. 16 (Article 17 ICCPR), 8 Apr. 1988, para. 3 (noting that "[t]he term 'unlawful' means that no interference can take place except in cases envisaged by the law" and that "[i]nterference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant".)

38 Report of the UN Special Rapporteur on Counter-Terrorism, UN Doc. A/HRC/34/61, 21 Feb. 2017, para. 36.

39 Malone v. United Kingdom, European Court of Human Rights, App. No. 8691/79, 2 Aug. 1984, para. 67 ("Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident."); see also UN Human Rights Committee, General Comment No. 16, supra, at para. 4 (noting that "the expression 'arbitrary interference' can also extend to interference provided for under the law" and that "[t]he introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims, and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances").

> "[A] norm, to be characterized as a 'law,' must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public . . . . Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not."[40]

The requirements of accessibility and foreseeability are also reflected in the jurisprudence of the European Court of Human Rights ("ECtHR"):

> "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a law unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able — if need be with appropriate advice — to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[41]

The UN General Assembly has recognized the application of the principle of legality to the surveillance context, resolving that the "surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and nondiscriminatory."[42]

Both the ECtHR and the Inter-American Court of Human Rights ("IACtHR") have also applied the principle of legality to the surveillance context. In Weber & Saravia v. Germany, the ECtHR elaborated on the "minimum safeguards that should be set out in statute law in order to avoid abuses of power" where the state conducts surveillance:

40 UN Human Rights Committee, General Comment No. 34 (Article 19 ICCPR), 12 Sept. 2011, para. 25.

41 Sunday Times v. United Kingdom, European Court of Human Rights, App. No. 6538/74, 26 Apr. 1979, para. 49.

42 UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc. A/RES/71/199, 19 Dec. 2016.

> "[1] the nature of the offences which may give rise to a [ ] [surveillance] order; [2] a definition of the categories of people liable to [be subject to surveillance]; [3] a limit on the duration of [surveillance]; [4] the procedure to be followed for examining, using and storing the data obtained; [5] the precautions to be taken when communicating the data to other parties; and [6] the circumstances in which recordings may or must be erased or the tapes destroyed."[43]

Similarly, in Escher et al. v. Brazil, the IACtHR held that surveillance measures "must be based on a law that must be precise." The Court further observed that the law must "indicate the corresponding clear and detailed rules, such as the circumstances in which this [surveillance] measure can be adopted, the persons authorized to request it, to order it and to carry it out, and the procedure to be followed."[44]

B. Intelligence Sharing and the Principle of Legality

Most intelligence sharing arrangements – both because the arrangements themselves are secret and the domestic laws that should govern them are non-existent – violate the principle of legality.

43 Weber & Saravia v. Germany, European Court of Human Rights, App. No. 54934/00, 29 June 2006, para. 95; see also Malone, supra, at para. 67 (noting that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence").

44 Escher et al. v. Brazil, Inter-American Court of Human Rights, Case 12.353, 2 Mar. 2006, para. 131.

1. Secret Intelligence Sharing Arrangements

Intelligence sharing arrangements are typically confidential and not subject to parliamentary scrutiny, often taking the form of secret memoranda of understanding directly between the relevant ministries or agencies. Such agreements may expressly state that they are not to be construed as legally binding instruments according to international law.[45] By doing so, the agreements can circumvent the requirement of ratification under the constitutional procedures and/or domestic laws of each member State as well as that of registration with the UN Secretariat in accordance with Article 102 of the UN Charter.

Case Study: The Five Eyes Alliance

As discussed above, one of the best known sharing arrangements is the Five Eyes alliance. The origins of the Five Eyes alliance stretch back to World War II, but the relationships between the five countries are formalized in the United Kingdom-United States Communication Intelligence Agreement ("UKUSA Agreement"), first signed in 1946 and amended numerous times thereafter. In 2010, the NSA declassified the 1946 agreement, along with other documents relating to its formation, implementation, and alteration.[46] As part of the 2010 series of declassifications, the NSA also declassified a 1956 revision of the UKUSA Agreement.[47] The UK, Australia and New Zealand have officially acknowledged that some version of the UKUSA Agreement remains in effect and continues to serve as the framework for intelligence sharing between the five countries.[48]

In July 2017, Privacy International, together with Yale Law School's Media Freedom & Information Access Clinic, filed a lawsuit against the NSA, the Office of the Director of National Intelligence, the Department of State, and the National Archives and Records Administration seeking access to the current and all prior versions of the UKUSA Agreement.[49]

45 See, e.g., Memorandum of Understanding Between the National Security Agency/Central Security Service (NSA/CSS) and the Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons, available at www.statewatch.org/news/2013/sep/nsa-israel-spy-share.pdf (noting that "this agreement is not intended to create any legally enforceable rights and shall not be construed to be either an international agreement or a legally binding instrument according to international law"). This agreement was first published by The Guardian on 11 September 2013. Glenn Greenwald et al., "NSA Shares Raw Intelligence Including Americans' Data with Israel", The Guardian, 11 Sept. 2013, https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

46 See UKUSA Agreement Release 1940-1956, NSA, 3 May 2016, https://www.nsa.gov/news-features/declassified-documents/ukusa/.

47 See UKUSA Agreement, para. 11. 10 Oct. 1956, https://www.nsa.gov/news-features/declassifieddocuments/ukusa/assets/files/new_ukusa_agree_10may55.pdf (indicating that the Agreement "supersedes all previous Agreements between U.K. and U.S. authorities in the [communications intelligence] COMINT field").

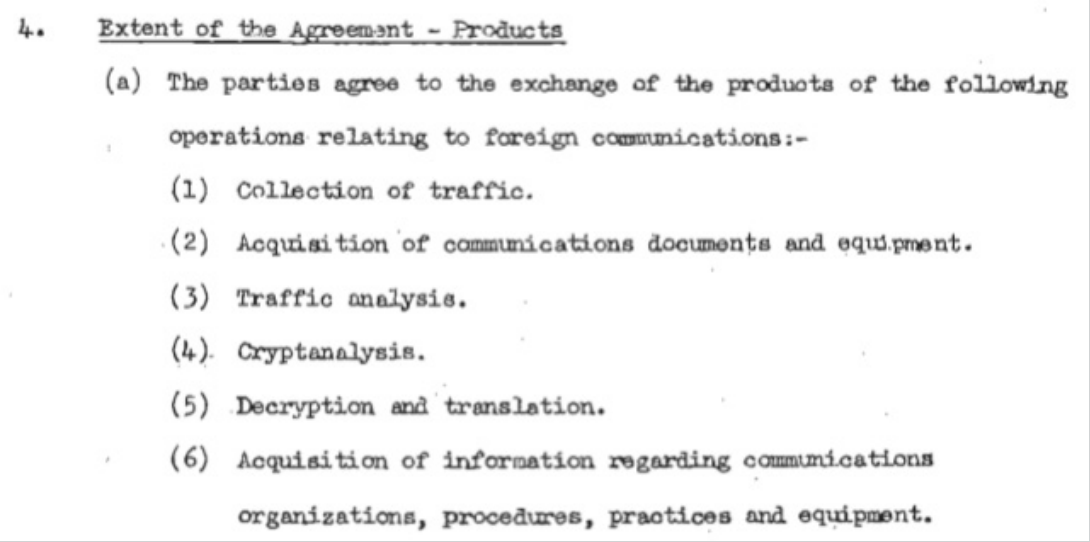
48 See "International Partners: How Sharing Knowledge and Expertise with Other Countries Helps Us Keep the UK Safe", GCHQ, 29 Sept. 2016, https://www.gchq.gov.uk/features/%20international-partners; "UKUSA Allies", Australian Signals Directorate, https://www.asd.gov.au/partners/allies.htm; "UKUSA Allies", Government Communications Security Bureau, 6. Dec. 2016, https://www.gcsb.govt.nz/about-us/ukusa-allies/.

49 See "MFIA Clinic Files Lawsuit in Five Eyes Alliance Case", Yale Law School, 6 July 2017, https://law.yale.edu/yls-today/news/mfia-clinic-files-lawsuit-five-eyes-alliance-case.

In response to our lawsuit, the NSA released new appendices to the UKUSA Agreement dating from 1959-61.[50] The 1956 version of the UKUSA Agreement, together with the 1959-61 appendices, is the most recent version of the agreement to have been made public.[51]

It is difficult to believe that this version of the UKUSA Agreement is the current agreement governing the Five Eyes alliance, particularly given how both communications methods and the nature of signals intelligence have changed dramatically since the late 1950s. In fact, the 1956 version of the UKUSA Agreement itself acknowledged that a reappraisal of the 1946 version of the agreement was necessary, in part, due to "the passage of time which has made out of date much of the detail contained in the Agreement." Indeed, in response to our lawsuit, the State Department has disclosed records suggesting that implementation of the UKUSA Agreement underwent amendments in the 2000s.[52]

Although we know little about the current UKUSA Agreement governing the Five Eyes alliance, the declassified versions of the agreement reveal a highly integrated vision of sharing between the five countries. Pursuant to the 1956 version of the UKUSA Agreement, the countries agree to the presumption of unrestricted exchange of signals intelligence as well as the methods and techniques related to signals intelligence operations. Paragraph 4 of the Agreement states that the "parties agree to the exchange of the products" of certain "operations relating to foreign communications," including "(1) Collection of traffic. (2) Acquisition of communications documents and equipment. (3) Traffic analysis. (4) Cryptanalysis. (5) Decryption and translation."[53] Paragraph 5 of the Agreement further provides for the parties to "exchange . . . information regarding methods and techniques involved in the operations" relating to foreign communications.[54]



4. Extent of the Agreement - Products

(a) The parties agree to the exchange of the products of the following operations relating to foreign communications:-

(1) Collection of traffic.

(2) Acquisition of communications documents and equipment.

(3) Traffic analysis.

(4) Cryptanalysis.

(5) Decryption and translation.

(6) Acquisition of information regarding communications organizations, procedures, practices and equipment.

Screenshot of a provision of the 1956 version of the UKUSA Agreement

50 The appendices can be found in Annex IV.

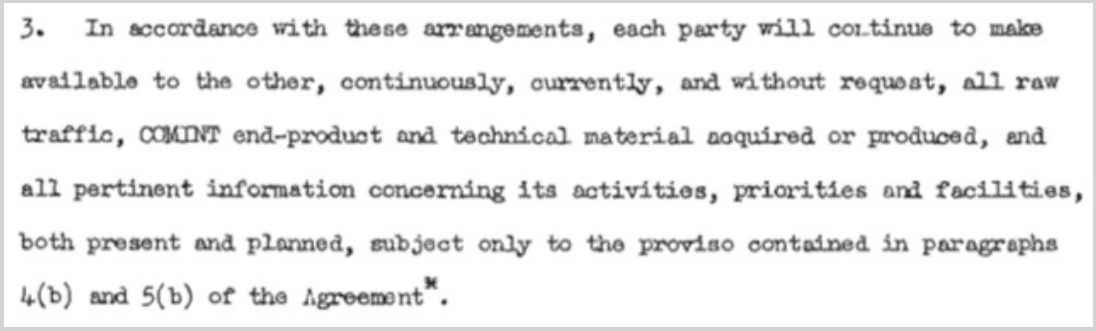
51 It is unclear whether other elements of the UKUSA Agreement, beyond the released appendices were also revised between 1956 and 1961.

52 These records can be found in Annex IV.

53 UKUSA Agreement para. 4(a), 10 Oct. 1956.

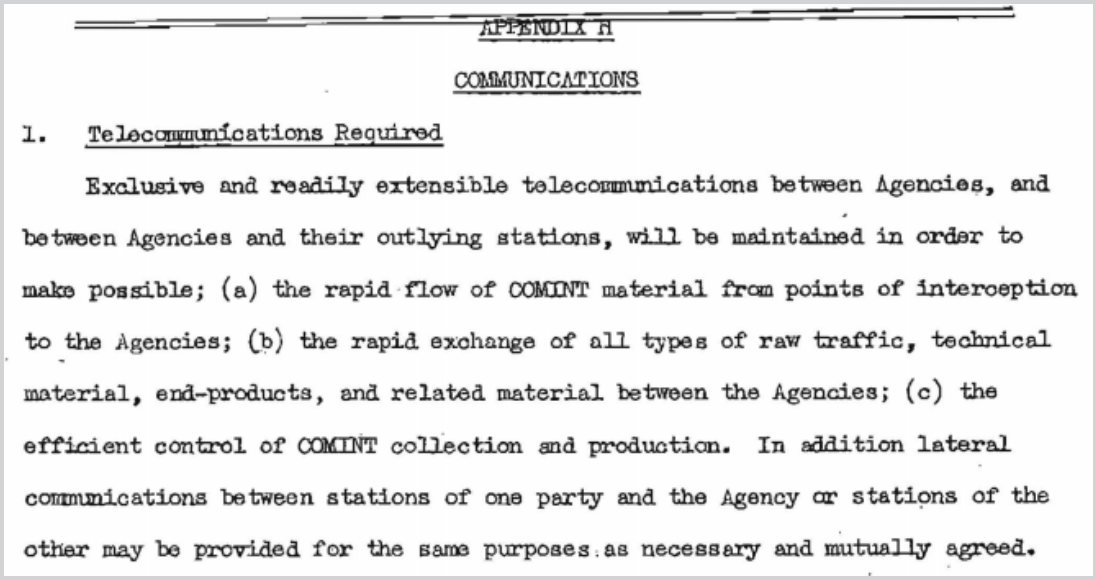
54 Id. at para. 5(a).

For the exchange of foreign communications products," paragraph 4 of the Agreement provides that "[s]uch exchange will be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party and with the agreement of the other" and that "[i]t is the intention of each party to limit such exceptions to the absolute minimum." The Agreement also provides, in an appendix articulating "General Principles of Collaboration on COMINT Production and Collection", that "[i]n accordance with these arrangements, each party will continue to make available to the other, continuously, currently, and without request, all raw traffic, COMINT end-product and technical material acquired or produced, and all pertinent information concerning its activities, priorities and facilities, both present and planned, subject only to" provisos contained in the Agreement.[55] In a separate appendix titled "Communications", the parties indicate their intent to maintain "[e]xclusive and readily extensible telecommunications . . . in order to make possible; (a) the rapid flow of COMINT material from points of interception to the Agencies; (b) the rapid exchange of all types of raw traffic, technical material, end-products, and related material between the agencies; (c) the efficient control of COMINT collection and production."[56]



3. In accordance with these arrangements, each party will continue to make available to the other, continuously, currently, and without request, all raw traffic, COMINT end-product and technical material acquired or produced, and all pertinent information concerning its activities, priorities and facilities, both present and planned, subject only to the proviso contained in paragraphs 4(b) and 5(b) of the Agreement*.

Screenshot of a provision of Appendix C to the 1956 version of the UKUSA Agreement



APPENDIX H

COMMUNICATIONS

1. Telecommunications Required

Exclusive and readily extensible telecommunications between Agencies, and between Agencies and their outlying stations, will be maintained in order to make possible; (a) the rapid flow of COMINT material from points of interception to the Agencies; (b) the rapid exchange of all types of raw traffic, technical material, end-products, and related material between the Agencies; (c) the efficient control of COMINT collection and production. In addition lateral communications between stations of one party and the Agency or stations of the other may be provided for the same purposes as necessary and mutually agreed.

Screenshot of a provision of Appendix H to the 1956 version of the UKUSA Agreement

55 Id. at ap. C para. 3.

56 Id. at ap. H para. 1.

Case Study: Joint Defence Facility Pine Gap

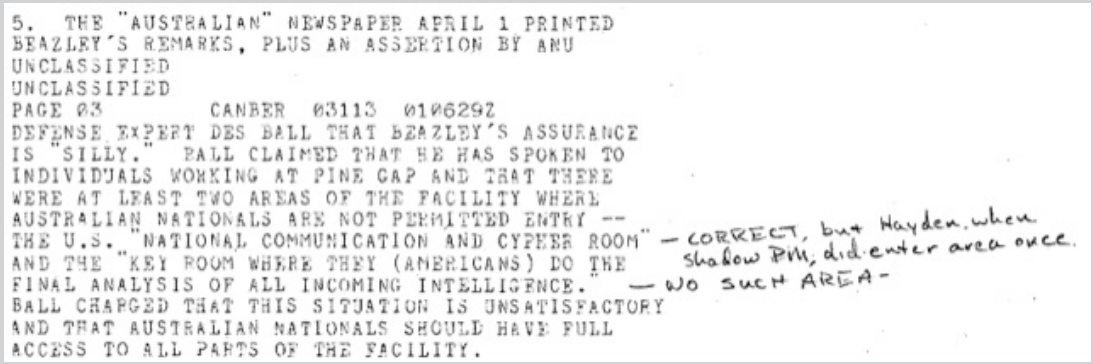
In response to Privacy International's lawsuit seeking access to the UKUSA Agreement, in December 2017, the State Department disclosed records relating to Joint Defence Facility Pine Gap. Pine Gap is a base located in Alice Springs, Australia and jointly operated by the US and Australia. From Pine Gap, the US controls satellites across several continents, which can conduct surveillance of wireless communications, like those transmitted via mobile phones, radios and satellite uplinks. The intelligence gathered supports both intelligence activities and military operations, including drone strikes.[57]

The disclosure includes what appears to be a 1985 State Department cable, which summarises public reporting and discussion of Pine Gap.[58] The cable includes a summary of remarks made by then-Australian defence minister Kim Beazley, including that the government "is fully aware of everything that takes place at the joint facilities and that [government] approval is required for any specific activity." The summary further quotes Beazley as saying: "Nothing happens at these facilities about which the government is unaware. Nothing can be done at these facilities without the acquiescence of the Australian government."

The cable then summarises remarks made by the defence expert, Desmond Ball, in response to Beazley:

> "Ball claimed that he has spoken to individuals working at Pine Gap and that there were at least two areas of the facility where Australian nationals are not permitted entry – the U.S. 'national communication and cypher room' and the 'key room where they (Americans) do the final analysis of all incoming intelligence.' Ball charged that this situation is unsatisfactory and that Australian nationals should have full access to all parts of the facility."

A handwritten comment in the margin of this text notes with respect to the "national communication and cypher room", "CORRECT, but Hayden when shadow PM, did enter area once." The handwritten comment then notes with respect to the "key room", "NO SUCH AREA".



5. THE "AUSTRALIAN" NEWSPAPER APRIL 1 PRINTED
BEAZLEY'S REMARKS, PLUS AN ASSERTION BY ANU
UNCLASSIFIED
UNCLASSIFIED
PAGE 03 CANBER 03113 0106292
DEFENSE EXPERT DES BALL THAT BEAZLEY'S ASSURANCE
IS "SILLY." BALL CLAIMED THAT HE HAS SPOKEN TO
INDIVIDUALS WORKING AT PINE GAP AND THAT THERE
WERE AT LEAST TWO AREAS OF THE FACILITY WHERE
AUSTRALIAN NATIONALS ARE NOT PERMITTED ENTRY --
THE U.S. "NATIONAL COMMUNICATION AND CYPHER ROOM" — CORRECT, but Hayden when shadow PM, did enter area once.
AND THE "KEY ROOM WHERE THEY (AMERICANS) DO THE
FINAL ANALYSIS OF ALL INCOMING INTELLIGENCE." — NO SUCH AREA -
BALL CHARGED THAT THIS SITUATION IS UNSATISFACTORY
AND THAT AUSTRALIAN NATIONALS SHOULD HAVE FULL
ACCESS TO ALL PARTS OF THE FACILITY.

Screenshot from 1985 State Department cable on Pine Gap

57 See "Pine Gap – An Introduction", Nautilus Institute, 21 Feb. 2016, https://nautilus.org/publications/books/australian-forces-abroad/defence-facilities/pine-gap/pine-gap-intro/; Jackie Dent, "An American Spy Base Hidden in Australia's Outback", NY Times, 23 Nov. 2017, https://www.nytimes.com/2017/11/23/world/australia/pine-gap-spy-base-protests.html.

58 This cable can be found in Annex IV.

2. Lack of Domestic Legislation

Our research suggests that most countries around the world lack domestic legislation governing intelligence sharing. In 2015, the UN Special Rapporteur on Counter-Terrorism stated in this regard that:

> "The absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority. Information concerning an individual's communications may be shared with foreign intelligence agencies without the protection of any publicly accessible legal framework and without adequate (or any) safeguards . . . . Such practices make the operation of the surveillance regime unforeseeable for those affected by it and are therefore incompatible with article 17 of the [International] Covenant [on Civil and Political Rights]."[59]

The 2017 report by the EU Agency for Fundamental Rights supports this conclusion in relation to most EU member states. The report notes that "[a]lmost all Member States (27 out of 28) have established international intelligence cooperation in their national legal frameworks", but that "[v]ery few . . . have explicitly articulated the modalities for both establishing and implementing international cooperation within the enabling laws."[60] Thus, at least in much of the EU, domestic laws governing international intelligence cooperation give intelligence agencies broad and vague powers to establish and implement such cooperation.

In several EU states, internal rules do govern intelligence sharing. However, these rules are drafted by the executive or by the agencies themselves and they are not publicly available. For example:

59 Report of the UN Special Rapporteur on Counter-Terrorism, UN Doc. A/69/397, 23 Sept. 2014, para. 44.

60 EU Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume II: field perspectives and legal update, Oct. 2017, p. 50.

- In **Belgium**, the guidelines for intelligence cooperation are classified and according to the Belgian Standing Intelligence Agencies Review Committee, the most important aspect of cooperation, i.e. the types of intelligence that can be shared with foreign services, is addressed only briefly in the guidance.[61]

- In the **Netherlands**, the internal guidelines are similarly classified although in 2016 the Dutch Review Committee on the Intelligence and Security Services published assessments of the procedures identifying significant shortcomings, which are discussed in Part V below.

Case Study: United Kingdom

In July 2013, Privacy International brought a lawsuit before the UK's Investigatory Powers Tribunal, challenging two aspects of the UK's surveillance regime revealed by the Snowden disclosures: (1) UK bulk interception of internet traffic transiting undersea fibre-optic cables landing in the UK and (2) UK access to the information gathered by the US through its various mass surveillance programs.[62] The Tribunal is a specialised court that hears complaints of unlawful surveillance by UK public bodies, including the security and intelligence services.

During the proceedings, the UK government referred to secret internal guidance governing its intelligence sharing with the US, which it presented to the Tribunal in a secret hearing. It later produced a 2-page "note" summarizing this guidance.[63] That note contained no heading and just a few paragraphs of text. It was unclear who drafted or adopted the note (and under what legal authority) or who had the power to amend it. It was unclear whether the note represented an actual policy, part of a policy, a summary of a policy, or a summary of submissions made by the UK government to the Tribunal in the closed hearing. It was also unclear whether it was binding in any way or simply a description of desirable practices.

In February 2015, the Tribunal determined that the UK government's access to information gathered via US bulk surveillance was unlawful prior to the legal proceedings before the Tribunal because the legal framework governing such access was secret. However, it found that the note described above was sufficient to render intelligence sharing lawful from the point of its disclosure.[64]

61 See EU Agency for Fundamental Rights, Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update, Oct. 2017, Belgium, http://fra.europa.eu/en/country-data/2017/country-studies-project-national-intelligence-authorities-and-surveillance-eu.

62 Nine other NGOs submitted similar complaints and the Tribunal subsequently joined the cases. The other nine NGOs are the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre and Liberty.

63 The text of this note is available in the Tribunal's 6 February 2015 judgment, available at https://privacyinternational.org/sites/default/files/2018-02/Liberty_Ors_Judgment_6Feb15.pdf.

64 Id.

In November 2016, the Investigatory Powers Act, which governs the surveillance powers of the UK's law enforcement agencies and security and intelligence services, was adopted. The Act only touches upon intelligence sharing in a few respects. First, section 9 provides that the UK may not request foreign authorities to "carry out the interception of communications sent by, or intended for" a person in the UK unless an appropriate warrant has been issued. Notably, this provision focuses on "requests" by the UK to foreign authorities to intercept particular communications; it does not appear to address other forms of intelligence sharing, including data the UK may not have explicitly "requested," such as the UK's direct and unfettered access to raw data intercepted in bulk or databases of material collected in bulk by foreign authorities.

Second, section 52 of the Act authorises interception "in response to a request made in accordance with a relevant international agreement" pursuant to several conditions, including where it is to obtain "information about the communications of an individual" outside or believed to be outside the United Kingdom. As above, this provision similarly focuses on "requests" by foreign authorities to the UK to intercept particular communications. Furthermore, the Act contains no provisions addressing "relevant international agreements" to share intelligence.

Third, several sections of the Act establish safeguards pertaining to the disclosure of material overseas obtained through interception or hacking (including as exercised in bulk). However, these "safeguards" appear to leave enormous discretion to the executive, by permitting it to apply certain rules pertaining to minimisation and destruction "to such extent (if any) as the issuing authority considers appropriate."[65]

In addition, the "note" described above has been substantially reproduced in the Interception of Communications Draft Code of Practice, a yet to be finalised policy document governing implementation of the Investigatory Powers Act. Both the note and the language in the Draft Code of Practice are obscurely drafted. For example, the Draft Code of Practice speaks of the UK intelligence agencies making a "request" for "unanalysed intercepted communications content (and secondary data)."[66] Again, it is unclear whether "request" covers all the scenarios where the intelligence agencies may access information obtained by foreign intelligence agencies, such as raw data intercepted in bulk or databases of material collected in bulk.

65 Sections 54, 130, 151, 192, Investigatory Powers Act 2016.

66 Interception of Communications Draft Code of Practice, Dec. 2017, paras. 9.33-9.40.

Case Study: Germany

In November 2016, Germany adopted the Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service (Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes).[67] The Act authorises the Federal Intelligence Service ("BND") to gather and process the communications of foreign nationals abroad. Sections 13-15 of the Act set out the general parameters for BND's intelligence cooperation with foreign agencies, including via intelligence sharing. Based on our research, the Act is the first and only attempt to date by a state to regulate in any detail, via primary legislation, intelligence cooperation through intelligence sharing.

The Act establishes several general principles that must guide intelligence sharing, including:

- Justifications for Cooperation: The BND may cooperate with foreign agencies only if it serves one of the following purposes: (a) to permit early identification of threats to Germany's internal or external security; (b) to preserve Germany's capacity to act; or (c) to obtain other information of relevance for Germany's foreign and security policy as defined by various relevant ministries. Within these broad purposes, the cooperation must only serve one or more of the following objectives: (1) to identify and tackle threats posed by international terrorism; (2) to identify and tackle threats posed by the proliferation of weapons of mass destruction and the illicit distribution of other types of arms; (3) to protect German armed forces and those of the states party to the cooperation; (4) to handle crises abroad; (5) to ensure the security of German nationals and the nationals of states party to the cooperation when they are abroad; (6) to obtain information relating to political, economic, or military operations abroad which are of foreign and security policy importance;
  or (7) to meet comparable cases.

- Exhaustion of Alternative Means: Cooperation will only be authorised to the extent that achieving the above stated purposes and objectives without such cooperation would be considerably more difficult or impossible.

- Written Requirement: BND cooperation with a foreign agency must be set out in a prior written agreement between the two agencies addressing (a) the cooperation objectives; (b) the content of the cooperation; and (c) the duration of the cooperation. The agreement must further include an agreement that: (a) data collected pursuant to cooperation may only be used for the purposes for which it was collected, and any use of the data must be compatible with fundamental rule of law principles; (b) the foreign agency will provide all information relating to its use of collected data upon request by the BND; and (c) the foreign agency will comply with a data deletion request by the BND.[68] The agreements are subject to the approval of the Federal Chancellery if the cooperation is with EU, European Economic Area or NATO member states. If cooperation

67 The Act is in German and there is currently no official English translation. Privacy International notes that its analysis is based on an unofficial translation of the Act.

68 See Thorsten Wetzling, Stiftung Neue Verantwortung, Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls, June 2017, p. 16, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

is with an agency of a country not party to these organisations, they require the direct approval of the Chancellor. The Parliamentary Control Committee shall be informed of all agreements.

- Automated Data Transmission, Storage, and Examination: Information, including personal data, may be shared with a foreign agency in an automated manner only to the extent that immediate transmission is necessary to reach the cooperation objectives and the automation process has been tested to ensure that certain data can be automatically deleted and not shared. That data includes data (1) improperly obtained; (2) concerning an EU institution, a public body of a member state, or citizens of the EU; and (3) which, if shared, would conflict with the national interests of Germany. Moreover, automatic sharing of data is to be recorded, and the log reviewed routinely to ensure compliance with the Act (all logs must be kept for two years and then deleted). These routine compliance checks must be conducted by a BND member who has the competence to become a judge.

While the principles noted above offer a number of safeguards, the Act also suffers from several shortcomings, including:

- International Human Rights Law as a Guiding Framework: Pursuant to the Act, cooperation agreements bind the parties to fundamental rule of law principles but not to international human rights law. Intelligence sharing (and other forms of intelligence cooperation) interfere with fundamental human rights. The Act should therefore clearly state that such cooperative activities shall be governed by international human rights law.

- Categories Justifying Intelligence Sharing: Pursuant to international human rights law, the principle of legality requires that relevant laws must meet certain minimum qualitative requirements of accessibility and foreseeability. Some of the justifications for cooperation under the Act are so vague (e.g. to handle crises abroad) or open-ended (e.g. in comparable cases) as to arguably violate the principle of legality.

- Circumventing Constraints on Surveillance: Intelligence sharing may lead to circumstances where states circumvent international or domestic constraints on direct surveillance by relying on their partners to obtain and then share information. The Act does not appear to explicitly prohibit the BND from using sharing arrangements to circumvent such constraints.

- Facilitating Serious Human Rights Abuses: The Act does not appear to articulate procedures for assessing whether information shared by the BND with other agencies may be used to facilitate serious human rights abuses. Similarly, the Act does not appear to articulate procedures for assessing information the BND accesses or receives through sharing, including whether it was obtained in violation of international law or raises reliability concerns.

V. Oversight and Intelligence Sharing

A. Oversight

International human rights law requires that any interference with the right to privacy "be attended by adequate procedural safeguards to protect against abuse." These safeguards "generally include independent prior authorization and/or subsequent independent review."[69] The UN General Assembly has therefore called on states "[t]o establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data."[70]

Independent oversight can take many forms. However, the UN Special Rapporteur on Counter-Terrorism has recommended, in the intelligence context, that "[a] n effective system of . . . oversight includes at least one civilian institution that is independent of both the intelligence services and the executive." In terms of the coverage of the oversight mechanisms, the Special Rapporteur observed that they should consider "all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices." The Special Rapporteur further recommended that oversight mechanisms should "have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates," and should "receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining

69 2014 Report of the UN Special Rapporteur on Counter-Terrorism, supra, at para. 45; see also UN Human Rights Committee, Seventh Periodic Report of the United Kingdom, supra, at para. 24 (recommending the State Party "[e]nsure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by . . . considering the establishment of strong and independent oversight mandates with a view to preventing abuses"); UN Human Rights Committee, Sixth Periodic Report of Canada, supra, at para. 10 (expressing concern "about the lack of adequate and effective oversight mechanisms to review activities of security and intelligence agencies and the lack of resources and power of existing mechanisms to monitor such activities" and recommending the State Party "[e]stablish oversight mechanisms over security and intelligence agencies that are effective and adequate and provide them appropriate powers as well as sufficient resources to carry out their mandate").

70 2016 UN General Assembly Resolution on the Right to Privacy in the Digital Age, supra, at para. 5(d); see also UN General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166, 18 Dec. 2014, para. 4; Report of the UN Special Rapporteur on Freedom of Expression, U.N. Doc. A/HRC/23/40, 17 Apr. 2013, para. 93 ("States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance mechanisms.").

documentation and other evidence." In addition, the Special Rapporteur further indicated that oversight mechanisms should "publish (annual) reports describing [their] activities and findings" and "as appropriate, incidental reports describing specific investigations."[71]

International human rights bodies have also emphasised prior independent authorisation – preferably judicial – as a key mechanism for "ensur[ing] the effectiveness and independence of a monitoring system for surveillance activities".[72] The UN Human Rights Committee has further recognised the importance of prior independent authorisation in the context of intelligence sharing, indicating that "robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities" should include "providing for judicial involvement in the authorisation of such measures in all cases".[73]

The ECtHR has similarly indicated that prior independent authorisation is a minimum safeguard to protect the right to privacy, particularly in the surveillance context. It has noted that "[i]n a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[74]

The Inter-American Commission of Human Rights Special Rapporteur for Freedom of Expression has also observed that "decisions to undertake surveillance activities that invade the privacy of individuals must be authorized by independent judicial authorities, who must state why the measure is appropriate for the accomplishment of the objectives pursued in the specific case; whether it is sufficiently restricted so as not to infringe upon the right in question more than necessary; and whether it is proportionate in relation to the interests pursued."[75]

71 Report of the Special Rapporteur on counter-terrorism, Compilation of good practices, supra, at Practices 6-7.

72 UN Human Rights Committee, Concluding Observations on the Fifth Periodic Report of France, UN Doc. CCPR/C/FRA/CO/5, 17 Aug. 2015, para. 12.

73 UN Human Rights Committee, Seventh Periodic Report of the United Kingdom, supra, at para. 24.

74 Zakharov, supra, at para. 233 (citing Klass and Others v. Germany, European Court of Human Rights, App. No. 5029/71, 6 Sept. 1978, paras. 55-56); see also Szabó, supra, at para. 77 ("[I]n this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny.").

75 Office of the Special Rapporteur for Freedom of Expression, Inter-American Commission on Human Rights, Freedom of Expression and the Internet, 31 Dec. 2013, para. 165.

B. Intelligence Sharing and Oversight

As a general matter, there is an alarming lack of effective oversight of secret surveillance in a range of countries around the world. As noted by the UN High Commissioner for Human Rights:

> "[A] lack of effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods. While these safeguards may take a variety of forms, the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law."[76]

In particular, there is a significant oversight gap when it comes to intelligence sharing practices. This gap has also been observed by a range of international human rights bodies. For example, in a 2017 report, the EU Agency for Fundamental Rights noted how "[v]ery few Member States allow expert bodies to assess international agreements and/or cooperation criteria" establishing intelligence sharing either ex ante or ex post.[77]

As a result, human rights bodies have repeatedly emphasised the importance of and called for effective oversight of intelligence sharing arrangements. In Szabó and Vissy v. Hungary, the ECtHR noted:

> "The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."[78]

76 UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age, supra, at para. 37.

77 EU Agency for Fundamental Rights, Surveillance by intelligence services, supra, at p. 51.

78 Szabó and Vissy v. Hungary, European Court of Human Rights, App. No. 37138/14, 12 Jan. 2016, para. 78.

The UN Human Rights Committee has accordingly recommended a number of states put in place "effective and independent oversight mechanisms over intelligence-sharing of personal data".[79] And the Council of Europe Commissioner for Human Rights has recommended that intelligence oversight bodies be mandated to scrutinise the human rights compliance of security service co-operation with foreign bodies, including co-operation through the exchange of information.[80]

Privacy International Campaign on Intelligence Sharing Oversight

In September 2017, Privacy International (in partnership with 40 national civil society organisations) wrote to oversight bodies in 42 countries as part of a project to increase transparency around intelligence sharing and to encourage oversight bodies to scrutinise the law and practice of intelligence sharing in their respective countries. The full list of oversight bodies we contacted is contained in Annex I and the full list of our organisational partners is contained in Annex II.[81]

In our letter to oversight bodies, we asked the following questions:

- Is the government and/or are the intelligence agencies required to inform you about intelligence sharing arrangements they have made with other governments?
- Does your mandate include independent oversight of the intelligence sharing activities of your government?
- Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?
- Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government?
- Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government?[82]

79 UN Human Rights Committee, Seventh Periodic Report of Sweden, supra, at paras. 36-37; see also UN Human Rights Committee, Concluding Observations on the Initial Report of Pakistan, supra, at para. 35; UN Human Rights Committee, Seventh Periodic Report of the United Kingdom, supra, at para. 24; UN Human Rights Committee, Sixth Periodic Report of Canada, supra, at para. 10.

80 Council of Europe Commissioner for Human Rights, Democratic and effective oversight of national security services, 2015, recommendation 5, https://rm.coe.int/1680487770.

81 For a map, which illustrates the countries included in the campaign, go to https://privacyinternational.carto.com/builder/28fccac2-3349-46e5-91bd-fd676d0efe1f/embed.

82 Our letter to the Canadian oversight bodies included two additional questions: (1) What, if anything, do you see as the primary current impediment to your capacity to substantively review intelligence-sharing activities of the agencies you oversee? and (2) To what extent is the Minister of National Defence involved in the negotiation, approval or internalization of intelligence-sharing agreements with foreign agencies or governments.

To date, we have received responses from oversight bodies in 21 countries: Australia, Austria, Belgium, Canada, Denmark, Estonia, Finland, France, Germany, Hungary, New Zealand, the Netherlands, Norway, Romania, Slovenia, Spain, Sweden, Switzerland, the UK and the US. All of the responses can be found in Annex III.

We have not received responses from oversight bodies in the following countries: Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Georgia, Greece, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Macedonia, Montenegro, Poland, Portugal, Slovakia, Spain, and Ukraine.

C. Trends and Concerns in the Oversight of Intelligence Sharing

Below, Privacy International outlines some key trends and concerns related to the oversight of intelligence sharing based on the responses we received to our letters to oversight bodies. All of the responses can be found in Annex III.

1. Access to Intelligence Sharing Arrangements

In some countries, intelligence agencies have no legal obligation to inform oversight bodies of the intelligence sharing arrangements into which they enter. For example:

- In **Estonia**, the Chancellor of Justice noted that "neither the government nor the intelligence agencies are required to inform the Chancellor of Justice about intelligence sharing arrangements they have made with other governments."

- In **Finland**, the Office of the Parliamentary Ombudsman responded: "The government or the public authorities concerned are not obliged spontaneously to inform the Parliamentary Ombudsman about intelligence sharing arrangements they have made with other governments."

- In **France**, the Commission nationale de contrôle des techniques de renseignement (National Commission for Oversight of Intelligence Gathering) indicated that the law places no explicit obligation on the government to inform the Commission of intelligence sharing ("[s]'agissant en particulier des échanges de renseignements entre le gouvernement français et des gouvernements étrangers, la loi n'a pas . . . fait explicitement obligation au gouvernement français d'informer la commission en cas d'échanges").

In other countries, while there are no explicit legal provisions requiring intelligence agencies to inform oversight bodies about intelligence sharing arrangements, oversight bodies have expressed the view that they can obtain such information under more general provisions requiring that the agencies furnish information or providing the bodies with powers to access information. For example:

- In **Australia**, the Inspector-General of Intelligence and Security responded that the agencies provide "all relevant policies and guidelines for the exchange of information with foreign authorities" and deemed that the "agencies have sound frameworks for the approval and conduct of intelligence sharing activities."

- In **Belgium**, the agencies have the legal obligation to send to the Belgian Standing Intelligence Agencies Review Committee all documents, directives and guidelines that regulate the actions of the members of the agencies. Arrangements between domestic agencies, such as a Memorandum of Understanding, are considered to be such directives. However, it is not clear from the response whether this includes arrangements between agencies in different countries.

- In the **Netherlands**, the Review Committee on the Intelligence and Security Services ("CTIVD") indicated: "The intelligence agencies are by law (article 73, Intelligence and Security Services Act 2002) obliged to furnish all information the [CTIVD] deems necessary for a proper performance of its duties. The CTIVD is also given the right to immediate access to all information. In practice, our investigators can access any processed data directly, including intelligence sharing arrangements."

- In **New Zealand**, the Inspector-General of Intelligence and Security noted that "there is no legislative provision requiring the GCSB [the Government Communications Security Bureau] or NZSIS [the New Zealand Security Intelligence Service] (or any other government body) to proactively inform the Inspector-General about current or new intelligence sharing arrangements with other governments or foreign agencies." However, the Inspector-General noted that she has "broad rights of access to all agency information which can, as necessary, include access to NZSIS or GCSB's intelligence sharing arrangements with other countries and foreign agencies."

- In **Norway**, the agencies "are not required by law to inform the [Parliamentary Intelligence Oversight] Committee about new intelligence sharing arrangements", but "the Committee may however demand access to the services' archives and registers, including information about arrangements the services have made with other governments/agencies."

- In the **United Kingdom**, the Investigatory Powers Commissioner indicated that he interprets the provisions of the Investigatory Powers Act (sections 208 and 235) as requiring the agencies provide his office "with all information necessary to enable us to conduct our oversight function."

Only the oversight body of one country – **Canada** – indicated that the intelligence agencies are required by law to provide them access to intelligence sharing arrangements.

- In **Canada**, the Security Intelligence Review Committee ("SIRC") stated: "According to section 17 of the [Canadian Security Intelligence Service] CSIS Act, SIRC must be provided with a copy of any written arrangement that CSIS enters 'with the government of a foreign state or an institution thereof or an international organization of states or an institution thereof.'"

In **Sweden**, intelligence agencies must inform the oversight bodies of the principles underpinning forms of cooperation with foreign agencies, although the law does not explicitly require they disclose the written arrangements of such cooperation.

- In **Sweden**, the State Inspection for Defence Intelligence Activity ("SIUN") noted that the ordinance on defence intelligence services (2000:131) requires that the defence intelligence authorities inform SIUN of the principles applicable to cooperation in intelligence issues with other countries and international organisations, as well as indicating with which countries and organizations such cooperation is taking place. Moreover, the ordinance further requires that the authorities, after the cooperation has been established, inform SIUN about the scope of the cooperation. The authorities may further inform SIUN, about the results, experience and continued direction of such cooperation.

2. Independent Oversight

As discussed above, international human rights law requires that any interference with the right to privacy "be attended by adequate procedural safeguards to protect against abuse." These safeguards "generally include independent prior authorization and/or subsequent independent review."[83]

83 2014 Report of the UN Special Rapporteur on Counter-Terrorism, supra, at para. 45; see also UN Human Rights Committee, Seventh Periodic Report of the United Kingdom, supra, at para. 24 (recommending the State Party "[e]nsure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by . . . considering the establishment of strong and independent oversight mandates with a view to preventing abuses"); UN Human Rights Committee, Sixth Periodic Report of Canada, supra, at para. 10 (expressing concern "about the lack of adequate and effective oversight mechanisms to review activities of security and intelligence agencies and the lack of resources and power of existing mechanisms to monitor such activities" and recommending the State Party "[e]stablish oversight mechanisms over security and intelligence agencies that are effective and adequate and provide them appropriate powers as well as sufficient resources to carry out their mandate").

The oversight body in one country – **France** – indicated that the law does not expressly provide the Commission with powers of oversight with respect to intelligence sharing.

- In **France**, the Commission nationale de contrôle des techniques de renseignement ("CNCTR") (National Commission for Oversight of Intelligence Gathering) indicated that it exercises oversight of surveillance techniques undertaken by the agencies, but that the law does not explicitly give them the mandate to oversee intelligence sharing ("[s]'agissant en particular des échanges de renseignements entre le government français et des gouvernements étrangers . . . la loi n'a pas expressément confié à la CNCTR de pouvoirs de contrôle").

a. Ex Ante Authorisation

None of the oversight bodies that replied to Privacy International indicated that they have powers to authorise decisions to share intelligence, either at a general level, or in specific circumstances. In fact, the process to authorise intelligence sharing appears often to bypass any independent authority. For example:

- In **Australia**, the Inspector-General of Intelligence and Security "does not review decisions to share intelligence prior to an agency sharing the intelligence, however the IGIS may be consulted by the relevant agency before it makes the decision to share."

- In **Finland**, "the Ombudsman does not have power to review decisions to share intelligence".

- In the **Netherlands**, the Intelligence and Security Services Act 2002 allows Dutch intelligence agencies to share information with foreign agencies but the relevant minister must give permission. A request must provide an accurate description of the required information and the reasons for providing it. Further a record must be kept of the intelligence cooperation provided.[84]

b. Ex Post Monitoring

Many of the oversight bodies that responded to Privacy International's letter discussed various powers they have to conduct ex post monitoring of the intelligence sharing activities of their agencies. In particular, they noted their powers to access information and to conduct inquiries and publish their results.

84 See EU Agency for Fundamental Rights, Country studies, supra, the Netherlands.

(i) Access to Information

Oversight bodies in a number of countries indicated that they have the power to access in full all relevant information about the intelligence sharing activities of the agencies. For example:

- In **Australia**, the Inspector-General of Intelligence and Security noted that she "has the power to access in full all relevant information about the intelligence sharing activities of the [Australian intelligence community] AIC."

- In **Belgium**, the Standing Intelligence Agencies Review Committee noted that it "ha[s] full access to all premises, documents and computer systems."

- In **Canada**, the Security Intelligence Review Committee ("SIRC") stated: "As set out in the CSIS Act, SIRC has full access to any information under the control of CSIS. As a result, SIRC may examine all of CSIS's files and all of its activities–no matter how highly classified that information may be. The sole exception is Cabinet confidences (i.e., written and oral communications that contribute to the collective decision-making of Ministers)."

- In **Finland**, the Ombudsman indicated: "According to the Finnish Constitution (Section 111) the Ombudsman ha[s] the right to receive from public authorities or others performing public duties the information needed for their supervision of legality. This means that if the Ombudsman focuses his or her supervision on the co-operation of public authorities with foreign authorities, he or she has access in full [to] all relevant information about the intelligence sharing activities."

- In the **Netherlands**, the Review Committee on the Intelligence and Security Services is "given the right to immediate access to all information."

- In **New Zealand**, the Inspector-General of Intelligence and Security noted: "I have broad rights of access to agency information as necessary to carry out all my statutory functions and duties."

- In **Norway**, the Parliamentary Intelligence Oversight Committee can "demand access to the services' archives and registers".

However, in most cases, the replies do not clarify whether the powers of the oversight body include accessing information provided by foreign agencies. This issue is likely to be sensitive, particularly in light of the third party rule / originator control principle.

One oversight body in one country – **France** – did indicate that it was prohibited from requesting this information.

- In **France**, the Commission nationale de contrôle des techniques de renseignement ("CNCTR") (National Commission for Oversight of Intelligence Gathering) indicated that it is prohibited by law from requesting access to information shared by foreign partners with the agencies ("le 4° de l'article L. 833-2 du [code de la sécurité intérieure] ne permet pas, à ce jour, à la CNCTR de demander un accès aux informations que les services de renseignement français pourraient obtenir de leurs homologues"), although the government could, on its own initiative, grant the Commission access to such information ("la loi n'interdit pas au gouvernement français de donner, de sa propre initiative, à la commission accès des informations obtenues de services de renseignement étrangers").

(ii) Powers to Conduct Inquiries

Some responses made reference to the powers entrusted to oversight bodies to conduct inquiries, which would be applicable also to monitor intelligence sharing. For example:

- In **Australia**, the Inspector-General of Intelligence and Security ("IGIS") stated: "Under the IGIS Act, the IGIS can conduct an inquiry into a matter based on a complaint, of the IGIS's own motion, or in response to a ministerial request. The IGIS Act establishes certain immunities and protections and provides for the use of strong coercive powers to compel the production of information and documents, to enter premises occupied or used by a Commonwealth agency, to issue notices to persons to attend before the IGIS to answer questions relevant to the matter under inquiry, and for the IGIS to administer an oath or affirmation when taking evidence."

- In **New Zealand**, the Inspector-General of Intelligence and Security can conduct an investigation upon a specific complaint, or as part of an own-motion inquiry. Furthermore, the Intelligence and Security Act 2017 gives the Inspector-General the following powers, in the context of an inquiry:

    - To require any person to provide any information, document or thing in that person's possession or control, that the Inspector-General considers relevant to an inquiry;

    - To receive in evidence any statement, document, information or matter that may assist the Inspector-General with an inquiry, whether or not that material would be admissible in a court of law;

    - To require disclosure to the Inspector-General of any matter, despite that information, document, thing or evidence being subject to an obligation of secrecy under an enactment or otherwise;

  - To summon persons the Inspector-General considers able to give information relevant to an inquiry, and;

  - To enter, at a reasonable time, any premises used by an intelligence and security agency.

- In the **UK**, the Investigatory Powers Commissioner, whose office was recently established pursuant to the Investigatory Powers Act 2016, provided an initial analysis of the kind of oversight activities his office is considering. He noted: "There are a number of possible approaches that could be taken to provide adequate oversight of sharing, including (but not limited to) – detailed analysis of sharing policies and any relevant undertakings set out contractually or in other agreements to assess whether these are adequate to protect individual rights; direct inspection of organisations not apparently covered by the IPA, but who are in receipt of material collected under IPA authorisation; agreements with partner oversight bodies that would shadow any sharing agreements, and, enable oversight to be carried out by partners on our behalf."

Some oversight bodies have published reports on their investigations, several of which address or touch upon intelligence sharing:

- In **Australia**, the Inspector-General on Intelligence and Security conducted an inquiry into the actions of Australian government agencies in relation to the rendition of Mr Mamdouh Habib, a dual Egyptian-Australian citizen, from 2001 to 2005. The report contains a number of relevant recommendations, including to review guidelines and policies of intelligence sharing with foreign agencies.[85]

- In **Canada**, the Security Intelligence Review Committee's 2011 review of "CSIS's Relationship with a Foreign Partner" contains recommendations to address the fact that "enhanced information-sharing presents a number of challenges, not the least of which is the need for agencies like CSIS to reconcile Canadian democratic values with international intelligence practices."[86] According to the summary of the review contained in the Committee's 2011-12 annual report, the Committee recommended that CSIS (1) "develop policy and direction on . . . practical assurances, such as when and how they should be sought, under whose authority, and how

85 Inspector-General of Intelligence and Security, Inquiry into the actions of Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005, 2011, http://www.igis.gov.au/sites/default/files/files/Inquiries/docs/habib-inquiry.pdf.

86 A summary of this report is available in Security Intelligence Review Committee, SIRC Annual Report 2011-2012: Meeting the Challenge, 30 Sept. 2012, http://www.sirc-csars.gc.ca/anrran/2011-2012/index-eng.html?wbdisable=true#sc2a-h. For a review of a specific case of information sharing, see Security Intelligence Review Committee, CSIS's Role in Interviewing Afghan Detainees (SIRC Study 2010-01), 4 July 2011, http://www.sirc-csars.gc.ca/pdfs/criad_20110704-eng.pdf.

this process should be documented in operational reporting"; (2) update its policy on caveats; and (3) "seek legal advice to assist in developing specific parameters" on sharing information about "minors and young people with foreign partners."[87]

- In the **Netherlands**, following a Parliamentary motion for an investigation into the cooperation of Dutch intelligence agencies with the NSA, the Review Committee on the Intelligence and Security Services investigated the agencies' implementation of cooperation policies and published a report.[88] The report includes an assessment of intelligence sharing practices and notes areas of concern including, inter alia, the lack of clarity around the authorisation process for cooperation and the lack of assessment of foreign agencies' systems of data protection. A subsequent report, also stemming from a Parliamentary motion calling for an investigation into cooperation between the Dutch intelligence agencies and the NSA, assesses the policies and practices of sharing "unevaluated data" (defined as "data that has not (yet) been assessed for relevance to the performance of the tasks of the" Dutch intelligence agencies", also referred to as "bulk").[89] The report concludes, inter alia, that the "present law does not include firm rules for the provision of unevaluated data to foreign services" and that the intelligence agencies lack "a written policy concerning what must be understood by unevaluated data and under what circumstances, how and when authorisation must be obtained".[90]

- In **New Zealand**, the Inspector-General of Intelligence and Security indicated in a response that she was "currently conducting a (publicly announced) inquiry into whether the New Zealand intelligence agencies had knowledge of or involvement in the CIA detention and interrogation program between 2001/09", which "necessarily involves looking at current and past intelligence sharing practices." She further noted that she would "report publicly at the conclusion of [her] inquiry." In her 2017 annual report, the Inspector–General also noted that she has been conducting "an examination of what policies and guidance have been developed and implemented by the NZSIS and GCSB, and are in place now, to ensure that their staff comply with New Zealand's domestic law and international obligations when cooperating with other nations."[91] She anticipated "reporting publicly on this inquiry in 2018."

87 SIRC Annual Report 2011-2012, supra.

88 Review Committee on the Intelligence and Security Services, Review Report on the Implementation of Cooperation Criteria by AIVD and MIVD, 2016 https://english.ctivd.nl/investigations/r/review-report-48/documents/review-reports/2016/12/22/index48.

89 Review Committee on Intelligence and Security Services, Review Report on the Exchange of Unevaluated Data by the AIVD and the MIVD, 2016, https://english.ctivd.nl/investigations/r/review-report-49/documents/review-reports/2016/12/22/index49.

90 Id. at III-IV.

91 Office of the Inspector-General of Intelligence and Security, Annual Report, For the year ended 30 June 2017, 1 Dec. 2017, 15, http://www.igis.govt.nz/assets/Annual-Reports/Annual-Report-2017.pdf.

- In **Norway**, the Parliamentary Intelligence Oversight Committee, in its 2016 annual report, criticised the Police Security Service for sharing personal data with a foreign agency, pointing out that "considerations of protection of [the person's] privacy must take precedence over the desire for satisfactory cooperation with the [country in question's] services".[92]

3. Collaboration Among Oversight Bodies

As intelligence agencies increasingly cooperate and share information, it would seem logical that oversight bodies also collaborate with each other to ensure effective oversight of intelligence sharing. However, there are clear sensitivities about such collaboration, as noted in the reply by the **UK's** Investigatory Powers Commissioner:

> "Cooperation between oversight bodies is something that I am committed to developing, however, it must be recognised that there are challenges due to the differing legislative regimes and issues around privacy and data sharing that will need to be explored. You will note that the Act specifically restricts me from doing anything that would undermine national security and, consequently, I am pursuing this work with care."

Less problematic is cooperation in the form of exchanging views, such as sharing best practices, including through gatherings of intelligence oversight mechanisms at international or regional levels. For example:

- According to the replies by the oversight bodies of Canada, New Zealand and the UK, a **Five Eyes Intelligence Oversight and Review Council** has been established, to discuss "issues of mutual relevance and share best practices" (from the response of the Office of the Communications Security Establishment Commissioner, Canada) with the potential of exploring areas of further cooperation (including possibly on joint investigation, see below). In this respect, the **UK** Investigatory Powers Commissioner stated, for example: "I have held extremely positive discussions with oversight bodies from the 'Five Eyes' countries, including on the oversight of intelligence sharing. Preliminary discussions have led to a proposal to form a review body whose objectives include exchange of views on subjects of mutual interest and concern, the sharing of best practice in oversight methodology, and exploring areas where cooperation on reviews and the sharing of results is appropriate."

92 Norwegian Parliamentary Oversight Committee, Annual Report 2016, https://eos-utvalget.no/english_1/annual_reports/content_3/text_1401199189882/1491375729127/annual2016en.pdf.

- In **Belgium**, the Belgian Standing Intelligence Agencies Review Committee also noted that it has "frequent contacts with intelligence oversight bodies of other, mainly European countries".

Beyond this general level of cooperation, there also appears to be some scope for conducting joint investigations.

- **Belgium, Denmark, Netherlands, Norway and Switzerland**. The 2016 annual report of the Dutch Review Committee on the Intelligence and Security Services ("CTIVD") noted a joint project, which began in 2015, "involving, in addition to the CTIVD, the Belgian, Danish, Norwegian and Swiss oversight bodies, [which] was developed further in the past year. All of the participating oversight bodies are conducting an investigation into the exchange of data on (alleged) jihadists, each from their own national context and within the framework of its own mandate."[93]

- The **New Zealand** Inspector-General of Intelligence and Security noted: "At a recent meeting of the newly established Five Eyes Intelligence Oversight and Review Council, the potential to carry out joint oversight projects was canvassed. I am actively pursuing possibilities for carrying out parallel investigations with foreign oversight bodies to examine specified operational activities or, possibly, both or all 'ends' of a particular intelligence agency activity carried out across national borders. Any such investigations or joint projects should result in public reports."

93 Review Committee on the Intelligence and Security Services, Annual Report 2016, https://english.ctivd.nl/documents/annual-reports/2017/07/24/index.

VI. Recommendations

To address the concerns outlined in this report, Privacy International makes the following recommendations:[94]

To Legislative Bodies:

- Establish, through primary legislation, publicly accessible legal frameworks governing intelligence sharing, which require:
    - Intelligence sharing agreements to be subject to approval by both executive and legislative bodies, and to be presumptively public;
    - Intelligence sharing agreements to permit information shared by foreign partners to be accessed by oversight bodies, notwithstanding the third party rule;
    - That international and domestic legal constraints that apply to direct surveillance by intelligence agencies apply equally to information obtained through intelligence sharing agreements;
    - Prior independent authorisation for sharing intelligence with a foreign partner;
    - Transparency as to the circumstances in which intelligence agencies will share information and the procedures governing such sharing, including limiting sharing to where it is in accordance with law, necessary, and proportionate, and articulating the process for authorising sharing;
    - Regular audits by oversight bodies of the manner in which foreign partners store, manage and use information that has been shared.

94 Many of these recommendations were adapted from Born et al., Making International Intelligence Cooperation Accountable, supra; Hans Born & Aidan Wills, Overseeing Intelligence Services: A Toolkit, supra.

- Establish, through primary legislation, publicly accessible legal frameworks governing intelligence sharing, which require:
    - Intelligence agencies to:
        - Conduct due diligence and risk assessments when sharing information. These obligations should encompass the following:
            - Determining whether there exists a credible risk that sharing information with a foreign partner will contribute to or facilitate the violation of human rights;
            - Determining whether there exists a credible risk that information shared by a foreign partner was obtained in violation of human rights.
        - Establish and maintain audit trails documenting, inter alia, authorisations to share information, the information shared, and the manner in which it was shared;
        - Establish internal mechanisms by which staff may disclose concerns regarding intelligence sharing, either by the intelligence agency where he or she works or by a foreign partner.
    - Independent oversight bodies that oversee the intelligence agencies to exercise their powers with respect to intelligence sharing and to have the mandate, inter alia, to:
        - Fully access information held by the intelligence services, including information related to intelligence sharing;
        - Undertake investigations on their own initiative;
        - Examine the allocation and use of financial resources for intelligence sharing, including for providing equipment and training to foreign partners;
        - Hire technological and other experts to assist them in understanding and assessing, inter alia, the systems used for sharing intelligence.
    - The executive to inform oversight bodies of all agreements to govern intelligence sharing when they are concluded or revised.

To the Executive:

- Before entering into agreements to share intelligence, conduct a review of the compatibility of such agreements with international and domestic law.

- Develop written agreements to govern intelligence sharing with foreign partners, which:

    - Mandate that any sharing of information be in compliance with international law, including international human rights and international humanitarian law;

    - Indicate that intelligence sharing shall be subject to scrutiny by oversight bodies;

    - Permit information shared by foreign partners to be accessed by oversight bodies, notwithstanding the third party rule;

    - Articulate procedures for reporting breaches of limitations ("caveats") placed on shared information (e.g. how the information may be stored, managed or used) and the resolution of disputes arising from such breaches – by both its intelligence agencies as well as foreign partners;

    - Are negotiated in consultation with specialist legal advisors with expertise in international and domestic law relevant to intelligence sharing.

- Share all agreements to govern intelligence sharing with oversight bodies when they are concluded or revised.

- Require heads of intelligence agencies to regularly report on intelligence sharing activities with foreign partners.

- Develop written and publicly available guidelines governing intelligence sharing, which address, inter alia, decisions relating to intelligence sharing that require authorisation and the procedures for authorisation.

- Maintain databases that track the human rights records of countries with which intelligence agencies share information and which, inter alia:

    - Contain information regarding, inter alia, reports by governments; regional and international organizations; national, regional and international human rights bodies; and civil society organisations regarding human rights violations;

    - Are developed in consultation with and made available to relevant government agencies and oversight bodies;

    - Are made available to the public consistent with national security.

To Intelligence Agencies:

- Develop written and publicly available internal policies on intelligence sharing that:

International and Domestic Legal Obligations

  - Mandate compliance with domestic and international law, including international human rights and international humanitarian law;

Outbound Sharing

  - Prohibit information sharing with foreign partners where there exists a credible risk that such sharing will contribute to or facilitate the violation of human rights;
  - Require and establish due diligence and risk assessment procedures for determining whether there exists a credible risk that sharing information with a foreign partner will contribute to or facilitate the violation of human rights;
  - Require the attachment of limitations ("caveats") when sharing information to ensure such information is not used in violation of domestic or international law or for improper purposes;
  - Establish procedures for monitoring adherence to and addressing breaches of limitations ("caveats"), including, inter alia, reporting breaches to oversight bodies;
  - Require the attachment of an assessment of the reliability of information when sharing such information with partner agencies;
  - Establish a continuing obligation to correct or update information shared with foreign partners as soon as practicable upon discovering errors or concerns regarding its reliability;

Inbound Sharing

  - Prohibit the use of information where there exists a credible risk that a foreign agency obtained it in violation of international law;
  - Require analysing the provenance, accuracy and verifiability of information shared by another agency;

- Mandate respect for limitations ("caveats") placed by partner agencies on shared information, which may ensure such information is not used in violation of domestic or international law or for improper purposes;

- Require notification to partner agencies of any breach of limitations ("caveats") placed by those agencies;

Record-Keeping

- Establish audit trails documenting, inter alia, authorisations to share information, the information shared, and the manner in which it was shared;

Training

- Require all staff, whose responsibilities relate to information sharing, to receive training on, inter alia:

    - Relevant domestic and international law, including international human rights and humanitarian law;

    - Identifying, reporting and mitigating risks to human rights;

    - Seeking authorisation for sharing information, establishing and maintaining relevant audit trails, and reporting obligations to oversight bodies;

Reporting to Oversight Bodies

- Require regular reporting to oversight bodies on, inter alia, authorisations to share information, the information shared, and the manner in which it was shared;

- Require reporting to oversight bodies where a foreign partner has breached a limitation ("caveat") as well as when it has breached a limitation placed by a foreign partner, including a report on any remedial actions the agency has taken or proposes to take;

- Require reporting to oversight bodies where the agency suspects or becomes aware that information shared with a foreign partner contributed to or facilitated the violation of human rights;

- Require reporting to oversight bodies where the agency suspects or becomes aware that information shared by a foreign partner was obtained in violation of international law, including a report on any remedial actions the agency has taken or proposes to take;

Whistleblowing

- Establish internal mechanisms by which staff may disclose concerns regarding intelligence sharing, either by the intelligence agency where he or she works or by a foreign partner;

- Permit staff to make protected disclosures concerning wrongdoing to oversight bodies;

- Provide ready access to specialist legal advisors with expertise in international and domestic law relevant to intelligence sharing.

To Oversight Bodies:

- Undertake regular investigations into intelligence agencies' policies and practices relating to intelligence sharing.

- Regularly review and evaluate, inter alia:

  - Intelligence agencies' compliance with relevant international and domestic law when sharing intelligence, agreements to share intelligence, and the agencies' own internal policies;

  - Intelligence agencies' due diligence and risk assessment procedures and practices related to intelligence sharing;

  - The limitations attached to information ("caveats") shared with foreign partners as well as intelligence agencies' procedures for monitoring adherence to and addressing breaches of limitations;

  - The limitations attached to information ("caveats") shared by foreign partners as well as intelligence agencies' procedures for monitoring adherence to and addressing breaches of limitations;

  - Intelligence agencies' training programs for staff whose responsibilities relate to intelligence sharing;

  - Executive involvement in intelligence sharing and the processes used to keep the executive apprised of intelligence sharing;

  - The executive's guidelines governing intelligence sharing and compliance with those guidelines.

- Review breaches of limitations ("caveats") by foreign partners and any remedial actions taken by the agencies and address whether further remedial action is necessary, including a potential review of the intelligence sharing agreement with such partners.

- Review breaches of limitations ("caveats") by its intelligence agencies and any remedial actions taken by the agencies and address whether further remedial action is necessary.

- Review reports by intelligence agencies where they suspect or become aware that information shared with a foreign partner contributed to or facilitated the violation of human rights and any remedial actions taken by the agencies and address whether further remedial action is necessary, including a potential review of the intelligence sharing agreement with such partners.

- Review reports by intelligence agencies where they suspect or become aware that information shared by a foreign partner was obtained in violation of international law and any remedial actions taken by the agencies and address whether further remedial action is necessary, including a potential review of the intelligence sharing agreement with such partners.

- Investigate protected disclosures concerning wrongdoing made by staff of an intelligence agency.

- Regularly publish reports on investigations and reviews into intelligence sharing.

- Cooperate with foreign oversight bodies in states with whom intelligence is shared, including, inter alia, establishing procedures for:

    - Informing each other of mutual areas of concern regarding intelligence sharing;

    - Requesting that a foreign oversight body investigate and share unclassified reports on specific issues of mutual concern relating to intelligence sharing.

Annex I – List of Oversight Bodies Contacted

Country	Oversight Body	Response?
Albania	Legal Issues, Public Administration and Human Rights Committee, Parliament of Albania	N
	National Security Committee, Parliament of Albania	N
Armenia	National Security Council of the Republic of Armenia	N
Australia	Independent National Security Legislation Monitor	N
	Inspector-General of Intelligence and Security	**Y**
	Parliamentary Joint Committee on Intelligence and Security	**Y**
Austria	Committee on Human Rights, Austrian Parliament	N
	Standing Subcommittee of the Interior Affairs Committee, Austrian Parliament	N
	Rechtsschutzbeauftragter, Federal Ministry for National Defence and Support	**Y**
	Rechtsschutzbeauftragter, Federal Ministry of the Interior	N
Azerbaijan	Commissioner for Human Rights	N
Belgium	**Belgian Standing Intelligence Agencies Review Committee**	**Y**
Bosnia & Herzegovina	Joint Security and Intelligence Committee for Oversight of the Intelligence – Security Agency of BiH	N
Bulgaria	Committee for Control of the Security Services, the Application and Use of the Special Intelligence Means and Data Access under the Electronic Communications Act	N
Canada	**Communications Security Establishment Commissioner**	**Y**
	Security Intelligence Review Committee	**Y**
Croatia	Republic of Croatia Ombudsman	N
	Council for Civilian Oversight of Security and Intelligence Agencies	N
Czech Republic	Permanent Commission on Oversight over the Work of the Security Information Service	N
Denmark	**Intelligence Services Committee**	**Y**
	Danish Intelligence Oversight Board	**Y**
Estonia	Security Authorities Surveillance Select Committee	N
	Chancellor of Justice	**Y**
	Estonian Data Protection Inspectorate	**Y**
Finland	**Parliamentary Ombudsman**	**Y**
France	**Commission nationale de contrôle des techniques de renseignement**	**Y**
	Délégation parlementaire au renseignement	N
Georgia	Defence Security Committee, Parliament of Georgia	N

Germany	**Federal Court of Justice**	**Y**
	G 10 Commission	**Y**
Greece	Standing Committee on National Defence and Foreign Affairs	N
Hungary	Committee on National Security	N
	National Authority Data Protection and Freedom of Information	**Y**
Iceland	National Security Council	N
Ireland	The Hon. Ms. Justice Marie Baker	N
	The Hon. Mr. Justice Brian McGovern	N
	His Honour Judge John Hannan Office of the Complaints Referee	N
	Minister for Justice and Equality	**Y**
Italy	Parliamentary Committee for the Security of the Republic	N
Republic of Korea	Intelligence Committee, National Assembly	N
Latvia	National Security Committee	N
Lithuania	Committee on National Security and Defence	N
Luxembourg	Parliamentary Control Commission for the Luxembourg Secret Service	N
Macedonia	Ombudsman of the Republic of Macedonia	N
	Committee for Supervising the Work of the Security and Counter Intelligence Directorate and the Intelligence Agency	N
Montenegro	Security and Defense Committee	N
The Netherlands	**Dutch Review Committee on the Intelligence and Security Services**	**Y**
	Standing Committee on the Interior, House of Representatives	N
	Committee on the Intelligence and Security Services, House of Representatives	N
New Zealand	**Inspector-General of Intelligence and Security, Parliament**	**Y (2)**
	Intelligence and Security Committee	**Y**
Norway	**Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee)**	**Y**
Poland	Komisja do Spraw Sluzb Specjalnych (KSS) SEJM	N
Portugal	Council for the Oversight of the Intelligence System of the Portuguese Republic	N
Romania	**The Joint Standing Committee for the exercise of parliamentary control over the activity of the Serviciul Roman de Informatii (SRI)**	**Y**
	The Joint Standing Committee for the exercise of parliamentary control over the activity of the Foreign Intelligence Service	**Y**
Slovakia	Special Oversight Committee for the Slovak Information Service, National Council	N

Slovenia	Commission for the Supervision of Intelligence and Security Services, National Assembly	N
	Court of Audit	N
	Human Rights Ombudsman	N
	Information Commissioner	**Y**
Spain	Comisíon de Interior, Congress of Deputies	N
	Comisíon de Interior, Senate	N
	Spanish Ombudsman	**Y**
Sweden	**Foreign Intelligence Court**	**Y**
	Statens Inspektion För Försvarsunderrättelseverksamheten (SIUN)	**Y**
	Swedish Commission on Security and Integrity Protection (Säkerhets- och integritetsskyddsnämnden)	N
Switzerland	**Federal Data Protection Commissioner**	**Y**
Ukraine	National Security and Defense Council of Ukraine	N
United Kingdom	Intelligence and Security Committee of Parliament	N
	Investigatory Powers Commissioner	**Y**
United States	Select Committee on Intelligence, House of Representatives	N
	Select Committee on Intelligence, Senate	N
	Committee on the Judiciary, House of Representatives	N
	Committee on the Judiciary, Senate	N
	Privacy and Civil Liberties Oversight Board	**Y**

Annex II – List of Partner Organisations

Country	Organisation/Individual
Australia	Australian Lawyers for Human Rights
	CryptoAUSTRALIA
	Digital Rights Watch
	Electronic Frontiers Australia
	Human Rights Law Centre
	NSW Council for Civil Liberties
Austria	epicenter.works
Belgium	La Ligue des droits de l'Homme
Canada	British Columbia Civil Liberties Association
	Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic
	Christopher Parsons, Research Associate, Citizen Lab at the Munk School of Global Affairs, University of Toronto
Croatia	Centre for Peace Studies
Denmark	IT-Politisk Forening
Estonia	Estonian Human Rights Centre
France	La Quadrature du Net
	Ligue de droits de l'Homme
	Fédération internationale des ligues des droits de l'Homme (FIDH)
Germany	Reporters without Borders, Germany
Republic of Korea	Korean Progressive Network Jinbonet
	Open Net Korea
	PSPD Public Interest Law Center
Hungary	Eötvös Károly Institute
Ireland	Digital Rights Ireland
	Irish Council for Civil Liberties
Italy	Italian Coalition for Civil Liberties and Rights (CILD)
	HERMES – Centro Studi per la trasparenza e i diritti umani in rete
New Zealand	Aotearoa New Zealand Human Rights Lawyers Association
Macedonia	Metamorphosis
Portugal	Associação D3 – Defesa dos Direitos Digitais
Romania	Asociația pentru Tehnologie și Internet
Slovakia	European Information Society Institute
Slovenia	Citizen D
Spain	Xnet
Sweden	Civil Rights Defenders
United Kingdom	Big Brother Watch
	Liberty
	Open Rights Group
United States	Center for Democracy and Technology
	Electronic Frontier Foundation
	Electronic Privacy Information Center
	New America's Open Technology Institute

Annex III – Responses Received from Oversight Bodies

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Ms Scarlet Kim
Legal Officer
Privacy International
62 Britton Street
LONDON EC1M 5UY
UNITED KINGDOM

Dear Ms Kim

I refer to your letter expressing concerns about lack of transparency in intelligence sharing arrangements between the Australian government and foreign governments, and seeking information about my office's oversight of intelligence sharing arrangements.

The Office of the Inspector-General of Intelligence and Security commenced in 1987 as a means of providing effective oversight of the Australian intelligence agencies. In the thirty years since then, the office has developed a systematic and wide-ranging oversight regime, giving assurance to the Australian government as to the legality and propriety of the activities of the Australian intelligence agencies.

The attached information addresses your specific questions.

Yours sincerely

Margaret Stone

Margaret Stone
Inspector-General

November 2017

FOI and Archives Act warning:
This is an exempt document under the *Freedom of Information Act 1982* and may be an exempt record under the *Archives Act 1983*. Consult the Inspector-General of Intelligence and Security on any FOI or Archives Act request.

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Response to questions raised by Privacy International – October 2017

1. *Is the government and/or the intelligence agencies required to inform the IGIS about intelligence sharing arrangements they have made with other governments?*

The IGIS has oversight of the agencies which comprise the Australian intelligence community (AIC). The IGIS does not have oversight of the government itself, or of government agencies outside the Australian intelligence community other than in particular circumstances (see below).

The AIC agencies have provided the IGIS with all relevant policies and guidelines for the exchange of information with foreign authorities. The IGIS is satisfied that AIC policies and guidelines comply with relevant Australian government legislation, the United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, of which Australia is a signatory, and have the approval of relevant Australian government ministers.

Examples of guidelines governing the activities of the Australian intelligence community include:

- Attorney-General's Guidelines[1]
- Rules to protect the privacy of Australians[2].

The IGIS is satisfied that AIC agencies have sound frameworks for the approval and conduct of intelligence sharing activities. Regular inspections of intelligence agency activities, promoting a compliance culture within the agencies, and encouraging agencies to report problems proactively has proved to be an effective way of providing independent assurance to the Prime Minister, senior ministers and Parliament as to whether Australia's intelligence and security agencies act legally and with propriety.

2. *Does the IGIS mandate include independent oversight of the intelligence sharing activities of the Australian government?*

The IGIS mandate is limited to oversight of the AIC, but, at the request of the Prime Minister, the IGIS can also inquire into intelligence or security matters relating to other Australian government agencies.

[1] Attorney-General's Guidelines are online at https://www.asio.gov.au/sites/default/files/Attorney-General's%20Guidelines.pdf
[2] The Privacy Rules are online at https://www.asd.gov.au/publications/broadcast/20121002-privacy-rules.htm

The role of the IGIS is established under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). Under the IGIS Act, the role of the IGIS is to assist Ministers in overseeing and reviewing the activities of the Australian intelligence agencies for legality and propriety and for consistency with human rights.

Section 15 of the *Intelligence Services Act 2001* (ISA) provides that the ministers responsible for ASIS, ASD and AGO must make written rules to regulate the communication and retention of intelligence information concerning Australian persons (privacy rules). The term 'Australian persons' includes citizens and certain permanent residents and companies. The rules regulate the agencies' communication of intelligence information concerning Australian persons to other Australian agencies and to foreign authorities, including Australia's closest intelligence partners. Communication to foreign authorities is also subject to additional requirements. The privacy rules are unclassified and listed on the agencies' websites.

Privacy rules require that agencies may only retain or communicate information about an Australian person where it is necessary to do so for the proper performance of each agency's functions, or where retention or communication is required under another Act.

The IGIS routinely inspects agencies' application of the privacy rules for compliance with requirements. Separately, if a breach of an agency's privacy rules is identified by the agency, the agency in question must advise the IGIS of the incident and the measures taken by the agency to protect the privacy of the Australian person, or Australian persons more generally. Adherence to this reporting requirement provides us with sufficient information upon which to decide whether appropriate remedial action has been taken, or further investigation and reporting back to the IGIS is required.

3. *Does the IGIS have the power to access in full all relevant information about the intelligence sharing activities of the Australian government?*

The IGIS has the power to access in full all relevant information about the intelligence sharing activities of the AIC. The IGIS carries out regular inspections of the intelligence agencies that are designed to identify issues of concern, including in the agencies' governance and control frameworks. Early identification of such issues may avoid the need for major remedial action. These inspections include our staff directly accessing electronic records and reviewing hardcopy documentation. Under the IGIS's inquiry powers, the IGIS can require a person to produce documents, but this is not routinely necessary.

4. *Does the IGIS have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of the Australian government?*

The IGIS does not review decisions to share intelligence prior to an agency sharing the intelligence, however the IGIS may be consulted by the relevant agency before it makes the decision to share. The IGIS cannot overturn any decision made by an Australian intelligence agency, but where

concerns are identified, such as a breach of the privacy rules, the IGIS will ask the relevant agency to examine their handling of the matter, bearing in mind the particular concerns, and provide the IGIS with the outcome of their review. If not satisfied with this the IGIS could launch an inquiry into the matter.

Under the IGIS Act, the IGIS can conduct an inquiry into a matter based on a complaint, of the IGIS's own motion, or in response to a ministerial request. The IGIS Act establishes certain immunities and protections and provides for the use of strong coercive powers to compel the production of information and documents, to enter premises occupied or used by a Commonwealth agency, to issue notices to persons to attend before the IGIS to answer questions relevant to the matter under inquiry, and for the IGIS to administer an oath or affirmation when taking evidence.

The Prime Minister may request the IGIS to inquire into intelligence or security matters relating to other Australian Government agencies, and the IGIS must comply with such request.[3]

5. *Does the IGIS cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of the Australian government?*

We frequently liaise with other accountability and integrity agencies, both in Australia and overseas. This liaison provides opportunities for us to discuss matters of mutual interest, learn from each other's practices and keep abreast of significant developments in other jurisdictions.

A separate Australian entity, the Independent National Security Legislation Monitor (INSLM), complements the IGIS role, by reviewing the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation on an ongoing basis. This includes considering whether legislation contains appropriate safeguards for protecting the rights of individuals, remains proportionate to any threat of terrorism or threat to national security or both, and remains necessary.[4]

6. *Please share any non-confidential work products reflecting answers above.*

An example of the IGIS's examination of the exchange of intelligence information by Australian government agencies can be found in the 2011 Inquiry into the actions of Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005. Of particular relevance are the IGIS recommendations 3, 4, 5 and 6. The inquiry is online at the following link:

http://www.igis.gov.au/sites/default/files/files/Inquiries/docs/habib-inquiry.pdf

Further examples of IGIS focus on the Australian intelligence agencies' compliance with the privacy rules can be found in the IGIS annual reports located online at the following link:

http://www.igis.gov.au/publications-reports/annual-reports

[3] Section 9(3) and 9(4) IGIS Act
[4] https://www.inslm.gov.au/about

PARLIAMENT *of* AUSTRALIA

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY
Parliament House, Canberra ACT 2600 | Phone: (02) 6277 2360 | Fax: (02) 6277 8594 | Email: pjcis@aph.gov.au

19 October 2017

Dr Gus Hosein
Executive Director
Privacy International

Dear Dr Hosein

Thank you for your letter dated 13 September 2017 in relation to intelligence sharing arrangements between governments.

The Committee has considered your letter and asked me to respond on its behalf. I have attached to this letter responses to your questions.

I appreciate your interest in this matter and I trust this information will be of assistance to your project.

If you require any further information about the role and functions of the Committee please contact the Committee Secretariat on +61 2 6277 2360 or by email to pjcis@aph.gov.au.

Yours sincerely

Andrew Hastie MP
Chair

Attachment – response to questions

Is the government and/or are the intelligence agencies required to inform you about intelligence sharing arrangements they have made with other governments?

Does your mandate include independent oversight of the intelligence sharing activities of your government?

The functions of the Committee are outlined under section 29 of the *Intelligence Services Act 2001* (the ISA) and include reviewing the administration and expenditure of the six Australian intelligence agencies and inquiring into other matters referred to the Committee by a responsible Minister or either House of the Parliament. There is no requirement for the government or the intelligence agencies to inform the Committee of intelligence sharing arrangements, or for the Committee to oversee intelligence sharing activities.

Additionally, subsection 29(3) of the *Intelligence Services Act 2001* contains a number of limitations on the functions of the Committee. Among others, the subsection states that the functions of the Committee do not include:

- reviewing the intelligence gathering and assessment priorities of the agencies;
- reviewing sources of information, other operational assistance or operational methods available to agencies;
- reviewing particular operations that have been, are being or are proposed to be undertaken by the agencies;
- reviewing information provided by, or by an agency of, a foreign government where that government does not consent to the disclosure of the information;
- reviewing an aspect of the activities of an agency that does not affect an Australian person;
- reviewing rules made by responsible Ministers regulating the communication and retention by agencies of intelligence information concerning Australian persons;
- conducting inquiries into individual complaints about the activities of agencies,
- reviewing the content of, or conclusions reached in, assessments or reports made by the Defence Intelligence Organisation or the Office of National Assessments, or reviewing the sources of information on which they are based.

However, the activities of the Australian intelligence agencies are subject to review by the Inspector-General of Intelligence and Security (IGIS), an independent statutory office holder appointed by the Governor-General under the *Inspector-General of Intelligence and Security Act 1986*. The purpose of the IGIS's review is to ensure that the agencies act legally and with propriety, comply with ministerial guidelines and directives and respect human rights. The IGIS's inquiries are conducted in private, but may be reported on in IGIS annual reports.

Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?

The Committee is empowered under Schedule 1 to the *Intelligence Services Act 2001* to require persons, including agency heads, to appear before the Committee to give evidence or to produce documents to the Committee. However, the Committee must not require a person or body to disclose to the Committee operationally sensitive information or information that would or might prejudice Australia's national security or the conduct of Australia's foreign relations.

Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government?

As noted above, the functions of the Committee under the *Intelligence Services Act 2001* do not include oversight of the intelligence sharing activities of the Australian government.

Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government?

The Committee meets privately with the IGIS on an annual basis as part of its review of the administration and expenditure of intelligence agencies, and on other occasions as required.

From: **BMLV.ZentrLtg.GrpRev.DiszBW.AbtLtg.BürRSB** rechtschutzbeauftragter@bmlvs.gv.at
Subject: Antwort: Letter/Briefing on Intelligence Sharing Oversight
Date: 17 October 2017 at 15:36
To: scarlet@privacyinternational.org

B

Information - Rechtsschutzbeauftragter

Gemäß § 57 Abs. 1 des Militärbefugnisgesetzes (MBG) ist zur Prüfung der Rechtmäßigkeit von Maßnahmen der nachrichtendienstlichen Aufklärung und Abwehr beim Bundesminister für Landesverteidigung und Sport ein Rechtsschutzbeauftragter mit zwei Stellvertretern eingerichtet. Diese Organe sind bei der Besorgung der ihnen nach dem MBG zukommenden Aufgaben unabhängig und weisungsfrei. Sie unterliegen der Amtsverschwiegenheit.

Das Mandat des Rechtsschutzbeauftragten umfasst die unabhängige Kontrolle der Aktivitäten der Organe der militärischen Aufklärung und Abwehr auf ihre Gesetzmäßigkeit sowie die Befugnis, Zugang zu allen relevanten Informationen und Entscheidungen zu haben und diese zu überprüfen. Dieses Mandat umfasst auch die Prüfung der in § 25 MBG geregelten Übermittlung von Daten (im weitesten Sinn) an ausländische öffentlich Dienststellen, internationale Organisationen und zwischenstaatliche Einrichtungen. Der Bundesminister für Landesverteidigung und Sport hat die gesetzliche Verpflichtung (§ 25 Abs. 6 MBG) alle Übermittlungen von Daten österreichischer Staatsbürger an die angeführten ausländischen Institutionen dem Rechtsschutzbeauftragten zu melden. Der Rechtsschutzbeauftragte hat dem Bundesminister für Landesverteidigung und Sport jährlich einen Bericht über seine (Prüfungs)Tätigkeit zu erstatten. Dieser hat den Bericht über Verlangen dem zuständigen ständigen Unterausschuss des Nationalrats zur Einsicht und Auskunftserteilung vorzulegen. Die Voraussetzungen für eine Genehmigung der Datenermittlung durch Organe der militärischen Aufklärung und Abwehr sind in den §§ 20 bis 22 MBG eingehend geregelt.

Die Unabhängigkeit und Weisungsfreiheit des Rechtsschutzbeauftragten und seiner Stellvertreter ist durch die Verfassungsbestimmung des § 57 Abs. 7 MBG garantiert. Eine Beschränkung der Befugnisse, Rechte und Pflichten des Rechtsschutzbeauftragten kann vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Mitglieder mit einer Mehrheit von zwei Drittel der abgegebenen Stimmen beschlossen werden (Verfassungsbestimmung des § 57 Abs. 7 MBG). Damit wird auch den einfachgesetzlichen Bestimmungen der Abs. 2 bis 6 des § 57 MBG und § 25 Abs. 6 MBG eine erhöhte Bestandskraft verliehen. Diese Institution ist somit in ihrer Unabhängigkeit und Weisungsfreiheit verfassungsrechtlich abgesichert.

Belgian Standing Intelligence Agencies Review Committee
FORUM - Leuvenseweg 48 B4 - B-1000 BRUSSELS, BELGIUM, EUROPE
T +32(0)2 286 29 11 F+32(0) 2 286 2999 www.comiteri.be - e-mail : info@comiteri.be

Q&A - PRIVACY INTERNATIONAL

1. *Is the government and/or are the intelligence agencies required to inform you about intelligence sharing arrangements they have made with their governments?*

   The agencies have the legal obligation to send to the Committee all documents, directives and guidelines that regulate the actions of the members of the agencies (Article 33, Review Act, 18 July 1991). Formal arrangements between the agencies, such as MOU[1], are considered to be such directives. However, if these MOU are concluded by other authorities (e.g. Ministers, …), the Committee has to direct its request to those authorities involved.

2. *Does your mandate include independent oversight of the intelligence sharing activities of your government?*

   The powers of the Review Committee make no exception for the sharing activities of the Belgian agencies. It oversees the legality, efficiency and coordination of all the actions of the agencies. Only for the seizure of documents related to an ongoing judicial investigation, a specific procedure is developed in the Review Act (Article 51). Of course the review itself is restricted to the Belgian agencies only. The independency of the Committee is defined in a structural way by law.

3. *Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?*

   The Committee and its investigation staff have important powers defined by law (Article 48 et seq.). They also have full access to all premises, documents and computer systems. Furthermore they can hear all staff members and even former staff members.

4. *Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government?*

   We do. Sharing intelligence is a sensitive matter but the review on it knows no specific regime or procedure. The Belgian law on the Intelligence agencies (Intelligence and Security Services Act of 30 November 1998) holds the obligation for the Intelligence agencies to sustain a collaboration with foreign services and this obligation can also be overseen by the Committee.

[1] Memorandum/-a of Understanding (MOU)

Belgian Standing Intelligence Agencies Review Committee
FORUM - Leuvenseweg 48 B4 - B-1000 BRUSSELS, BELGIUM, EUROPE
T +32(0)2 286 29 11 F+32(0) 2 286 2999 www.comiteri.be - e-mail : info@comiteri.be

5. Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government?

We do. On the whole we have very frequent formal and informal contacts with other oversight bodies in Belgium such as the 'Data Protection Authority', the 'Police Oversight Committee', the 'Ombudsman' and so forth …
We also have frequent contacts with intelligence oversight bodies of other, mainly European countries and with international instances like the FRA, DCAF,…

For the Committee,
Wouter DE RIDDER
Secretary

For more information and our public annual reports, please visit our website at www.comiteri.be

Communications Security Establishment Commissioner

The Honourable Jean-Pierre Plouffe, CD

Commissaire du Centre de la securite des telecommunications

L'honorableJean-Pierre Plouffe, CD

November 7, 2017

Dr. Gus Hosein
Executive Director
Privacy International

Micheal Vonn
Policy Director
BC Civil Liberties Association

Tamir Israel
Staff Lawyer
Samuelson-Glushko Canadian Internet
Policy & Public Interest Clinic (CIPPIC)

Christopher Parson
Research Associate
Citizen Lab at the Munk School of Global Affairs,
University of Toronto

Re: Oversight of intelligence sharing between your government and foreign governments

Dear Sirs and Madam:

Thank you for your letter of September 13, 2017 and for the opportunity to address some very important issues that you have inquired about.

I would like to preface my answers to your questions by clarifying my role and by providing a brief overview of some recent legislative developments that have the potential to significantly alter the security and intelligence review landscape that is the subject of your letter.

My role is to provide independent, external review of Communications Security Establishment (CSE) activities to determine whether they complied with the laws of Canada, including the *National Defence Act,* the *Charter of Rights and Freedoms* and the *Privacy Act.* I provide an annual report for Parliament-which is tabled by the Minister of National Defence, who is responsible to Parliament for CSE-about the activities of my office, including unclassified summaries of my reviews of CSE activities. My annual reports and other information about my office are provided on my web site: https://www.ocsec-bccst.gc.ca/en.

P.O. Box/C.P. 1474, Station "B" / Succursale «B»
Ottawa, Ontario K1P 5P6
Tel: 613-992-3044, Fax: 613-992-4096
info@ocsec-bccst.gc.ca

Canada currently has a number of review bodies that examine the activities of government organizations and agencies involved in national security operations, namely the Security Intelligence Review Committee (SIRC), the CSE Commissioner, and the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police (RCMP). These bodies are organization-specific and do not directly engage parliamentarians in their reviews. To address identified gaps in this structure, the Government of Canada recently passed legislation to establish a National Security and Intelligence Committee of Parliamentarians (NSICOP). The NSICOP will have a broad government-wide mandate to scrutinize any national security matter and will be empowered to perform reviews of national security and intelligence activities, including ongoing operations, and strategic and systemic reviews of the legislative, regulatory, policy, expenditure and administrative frameworks under which these activities are conducted. It will also conduct reviews of matters referred by a Cabinet minister, or discontinue a review if a minister deems its conduct to be injurious to national security. The Committee will be authorized to coordinate and collaborate with the individual review bodies within their respective mandates to minimize duplication and ensure effectiveness and efficiency in the broader review framework.

Most recently, the Government introduced a Bill (C-59) that aims to create a new review body-the National Security and Intelligence Review Agency-that would not only replace the current review bodies responsible for CSE and the Canadian Security Intelligence Service (CSIS), i.e., the CSE Commissioner and SIRC, respectively, but that would be responsible to review the security and intelligence activities of all federal Government departments and agencies. This Bill also proposes, *inter alia,* to establish an Intelligence Commissioner, who would fulfil a quasi-judicial oversight role in approving authorizations of certain CSE and CSIS activities prior to their conduct. The precise nature and modalities of the interactions among the various review and oversight bodies will depend on the form in which, and if, Bill C-59 passes into law. You may wish to consult the Bill as it currently is at first reading in Parliament.

Having provided these prefacing remarks, my answers to your questions follow. It is important to note that where your questions pertain to "your government," I have necessarily limited my answers to CSE, as that is the scope of my mandate.

Q1: ***Is the intelligence agency required to proactively inform you about intelligence sharing arrangements they are intending, or would prefer to make with other intelligence agencies or governments?***

No. The CSE Commissioner is mandated to review CSE's operational activities to verify their compliance with the law and that appropriate measures were taken to protect privacy. The very nature of *review* in this context implies after-the-fact examination of activities that have occurred. Consequently, while I appreciate receiving pertinent information at the earliest possible time, and while my office's review work aims to be forward-looking, and preventive in approach, in addition to retrospective, CSE has no obligation to inform the Commissioner's office in advance of activities or arrangements that are being contemplated or planned.

However, my approach to review is proactive and purposive, whereby I examine not only CSE's activities to verify whether they were conducted lawfully, but also CSE's policies,

procedures and practices to identify weaknesses or gaps that could increase the risk of non-compliance, and thereby seek to mitigate risk and strengthen the agency's culture of compliance. In fact, a number of my reports have included recommendations aimed specifically at taking preventive measures to help reduce the risk of non-compliance and to enhance privacyprotection.

Q2: ***Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?***

As set out in the *National Defence Act,* I have all the powers of a Commissioner under Part II of the *Inquiries Act,* including the power of subpoena, which gives me and my staff unfettered access to all CSE facilities, documents and personnel. As such, I can access all relevant information about the intelligence sharing activities of CSE.

Q3: ***Do you have sufficient power and resources to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government, including with respect to the substantive scope and proportionality of such sharing?***

I have sufficient resources to monitor and review CSE's intelligence-sharing decisions, arrangements and activities, and to undertake any investigations in relation to such sharing and to satisfy any concerns I may have. My office has conducted reviews specifically of CSE's information sharing with foreign entities and I continue to monitor these and related activities.

Q4. ***Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government? Are you able to share sufficient information with these other oversight bodies to provide adequate oversight and review?***

I have no explicit authority to collaborate with other review or oversight bodies. However, in the domestic realm, when reviewing CSE activities that involve another Government of Canada security and intelligence (S&I) or law enforcement agency, such as CSIS or the RCMP, I have taken the same approach as my predecessors in sharing pertinent information with the review body of the respective agency. As an example, within a five-year period my immediate predecessor and I have sent ten letters to the Chair of SIRC with information related to CSIS, for SIRC to follow up on as it deems appropriate.

In the international realm, I have participated in meaningful discussions with other review and oversight bodies within the "Five Eyes" community on a number of issues, including the sharing of information by intelligence agencies and the protection of privacy. These discussions have yielded a proposal to establish a forum through which review and oversight bodies of Five Eyes S&I organizations can discuss issues of mutual relevance and share best practices. This, in turn, should lead to an enhanced mutual awareness of key issues and challenges, such as privacy protection, and to more informed and consistent approaches being

taken across the Five Eyes S&I review community. This forum would also explore possible areas of cooperation on reviews and sharing of results, where and as appropriate.

Q5. ***What, if anything, do you see as the primary current impediment to your capacity to substantively review intelligence-sharing activities of the agencies you oversee?***

I have not identified any impediment to my substantively reviewing the intelligence sharing activities of CSE; however, as noted immediately above, formal authority to cooperate and share review-specific operational information with other review bodies would strengthen review capacity and effectiveness. Should Bill C-59 pass, the creation of a single agency to review national security activities across Government departments and agencies should resolve this issue.

Q6. ***To what extent is the Minister of National Defence involved in the negotiation, approval or internalization of intelligence-sharing agreements with foreign agencies or governments?***

This is a question that the Minister's office would be best situated to answer.

I trust my answers are clear and comprehensive. Please do not hesitate to contact me or my office if you have any further questions.

Sincerely,



The Honourable Jean-Pierre Plouffe, CD

c.c. The Honourable Pierre Blais, PC
Chairperson, SIRC

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

Office of the Chairman

Bureau du président

November 2nd, 2017

Dr. Gus Hosein
Executive Director
Privacy International

Micheal Vonn
Policy Director
BC Civil Liberties Association

Tamir Israel
Staff Lawyer
Samuelson-Glushko Canadian Internet
Policy & Public Interest Clinic (CIPPIC)

Christopher Parsons
Research Associate
Citizen Lab at the Munk School of Global Affairs,
University of Toronto

Re: Oversight of intelligence sharing between your government and foreign governments

Dear Sirs and Madam:

Thank you for your letter of September 13th and for the opportunity to respond to your questions which had also been addressed to my colleague, the Hon. Jean-Pierre Plouffe, C.D., Commissioner of the Communications Security Establishment (CSE).

I will begin by laying out my role as the Chair of the Security Intelligence Review Committee (SIRC). SIRC is an independent, external review body which reports to the Parliament of Canada on the operations of the Canadian Security Intelligence Service (CSIS). CSIS is Canada's security intelligence agency, responsible for investigating activities suspected of constituting threats to the security of Canada, and to reporting on these to the Government of Canada.

SIRC works to ensure that CSIS uses its powers legally and appropriately, in order to protect Canadians' rights and freedoms. SIRC provides an annual report for Parliament—which is tabled by the Minister of Public Safety, who is responsible to Parliament for CSIS. These are available on SIRC's website: http://www.sirc-csars.gc.ca.

However, as you are no doubt aware, the system of accountability for national security in Canada is in the midst of substantial change. In particular, there is a draft Bill before Parliament that, if

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
613 990-8441

passed unchanged, will create a new review body—the National Security and Intelligence Review Agency (NSIRA)—that would replace SIRC and the Office of the CSE Commissioner (OCSEC), and would be responsible for reviewing the security and intelligence activities of all Government departments and agencies.

Below you will find answers to your specific questions.

Q1: ***Is the intelligence agency required to proactively inform you about intelligence sharing arrangements they are intending, or would prefer to make with other intelligence agencies or governments?***

According to section 17 of the *CSIS Act*, SIRC must be provided with a copy of any written arrangement that CSIS enters "with the government of a foreign state or an institution thereof or an international organization of states or an institution thereof."

Q2: ***Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?***

As set out in the *CSIS Act*, SIRC has full access to any information under the control of CSIS. As a result, SIRC may examine all of CSIS's files and all of its activities—no matter how highly classified that information may be. The sole exception is Cabinet confidences (i.e., written and oral communications that contribute to the collective decision-making of Ministers).

Q3: ***Do you have sufficient power and resources to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government, including with respect to the substantive scope and proportionality of such sharing?***

SIRC has adequate resources to review CSIS's intelligence sharing practices and does so on an ongoing basis. SIRC's reviews of information sharing assess whether CSIS's information sharing practices are compliant with the laws of Canada, including the *CSIS Act*, the *Privacy Act*, as well as the *Security of Canada Information Sharing Act* (*SCISA*). SIRC also assesses those practices for compliance with the full range of applicable Ministerial Directions.

For your information, in addition to the review, "Ministerial Direction and CSIS's Directives on Intelligence Sharing," noted in your correspondence, SIRC recently conducted its first review of *SCISA*. I would also point you to SIRC's "Review of CSIS's Relationship with a Foreign Partner" in SIRC's 2011-2012 Annual Report. Summaries of these reviews are available in the annual reports on SIRC's website. You may also wish to consult SIRC's 2010 review, "CSIS's Role in Interviewing Afghan Detainees," the redacted version of which is on the website.

Q4. ***Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government? Are you able to share sufficient information with these other oversight bodies to provide adequate oversight and review?***

The *CSIS Act* does not provide SIRC the explicit authority to cooperate with other review or oversight bodies, either domestically or internationally. As indicated in the letter by the CSE Commissioner, internationally, SIRC has participated in discussions with OCSEC and other review and oversight bodies from the "Five Eyes" community. SIRC is optimistic that these discussions will contribute to greater awareness among the "Five Eyes" review and oversight community on issues of common concern, and may lead to forms of cooperation, as appropriate, in the future.

Q5. ***What, if anything, do you see as the primary current impediment to your capacity to substantively review intelligence-sharing activities of the agencies you oversee?***

SIRC has identified the lack of authority to share specific information with its domestic counterparts as an impediment to its capacity to review the activities of CSIS. This promises to be resolved with the creation of NSIRA as proposed in Bill C-59.

Q6. ***To what extent is the Minister of National Defence involved in the negotiation, approval or internalization of intelligence-sharing agreements with foreign agencies or governments?***

This is a question better suited for the Minister of National Defence's office.

Please do not hesitate to contact me or my office should you wish further clarification.

Sincerely,

Pierre Blais

PIERRE BLAIS, P.C.
Chair

c.c.: Hon. Jean-Pierre Plouffe, C.D.,
Commissioner of CSE

FOLKETINGET

Dr. Gus Hosein, Privacy International, og Jesper Lund, IT-Politisk Forening

Udvalget vedrørende
Efterretningstjenesterne
Christiansborg
DK-1240 København K
Tlf. +45 33 37 55 00

www.ft.dk
ft@ft.dk

28. september 2017

Ref. 13-000488-7

Kære Dr. Gus Hosein og Jesper Lund

Udvalget vedrørende Efterretningstjenesterne har modtaget Privacy Internationals og IT-Politisk Forenings brev af 13. september 2017, hvor man bl.a. spørger, om udvalgets opgaver indbefatter kontrol med informationsudvekslingsaktiviteter, og om udvalget samarbejder med andre kontrolinstanser i denne sammenhæng.

Udvalget vedrørende Efterretningstjenesternes formål og opgaver følger af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, jf. lovbekendtgørelse nr. 937 af 26. august 2014, link indsat herunder.

https://www.retsinformation.dk/Forms/R0710.aspx?id=164541

Udvalget kan ikke gå nærmere ind i en beskrivelse af udvalgets arbejde, end hvad der fremgår af lovgrundlaget.

Opmærksomheden henledes på, at der den 1. januar 2014 blev oprettet et Tilsyn med Efterretningstjenesterne, TET, som har til opgave at føre kontrol med, at PET og FE behandler oplysninger om fysiske og juridiske personer i overensstemmelse med de nærmere bestemmelser herom i lov om Politiets Efterretningstjeneste (PET) og lov om Forsvarets Efterretningstjeneste (FE) samt regler udstedt i medfør heraf. Tilsynets hjemmeside indeholder en nærmere beskrivelse af tilsynets formål og opgaver, jf. www.tet.dk.

Med venlig hilsen
på udvalgets vegne

[redacted]

1/1

tet

Tilsynet med Efterretningstjenesterne

Privacy International
62 Britton Street
London
United Kingdom

Dato: 29-09-2017
Sagsnr.: 2017-152-33
Dok.: 11910

Dear Dr. Gus Hosein

In reply to your letter from the 13th of September 2017.

I can inform you that the answers to all of your questions, and much more information about us, is available in our annual reports and our website.

The website is available in English and can be found here: http://www.tet.dk/en/

Our annual reports from 2015 will become available in English in the coming months.

In regards to your questions about intelligence sharing I can refer you to page 21 of our annual report from 2016 about the Danish Defence Intelligence Service and page 24 in our annual report from 2016 about the Danish Security and Intelligence Service.

Sincerely,

On behalf of The Danish Intelligence Oversight board

Emil Bock Greve
Acting Head of Secretariat

Side 1/1

Borgergade 28, 1.
DK-1300 København K
t 25 50 10 34
www.tet.dk

Chancellor of Justice

Dr Gus Hosein
Privacy International
Mr Kari Käsper
Eesti Inimõiguste Keskus
edin@privacyinternational.org

Your ref. 14.09.2017 No

Our ref. 30.10.2017 No 5-2/1704010

RE: Oversight of intelligence sharing between your government and foreign governments

Dear Sirs,

The mandate of the Chancellor of Justice guaranteeing fundamental rights and freedoms by agencies responsible for covert processing of personal data and supervision of that process is enacted in the Chancellor of Justice Act. The Act s. 1 (6) states that the Chancellor of Justice exercises supervision over observance of fundamental rights and freedoms in organisation of covert collection of personal data and information related thereto, processing, use and supervision thereof by all authorities of executive power in Estonia. The Act s. 11^1 says that the Chancellor of Justice has the right by virtue of office to access state secrets and classified information of foreign states in order to perform duties which have been assigned to him or her by the Constitution or Acts of the Republic of Estonia and by legislation issued on the basis thereof. However, the Act s. 11^1 (6) sets some restrictions on the performance of these tasks (please see below).

The Estonian law makes a clear distinction between the information exchanged by **security authorities** (e.g. for the prevention of terrorism, counter-intelligence operations, etc under the Security Authorities Act) and the information gathered by **surveillance agencies** under the Code of Criminal Procedure. The Chancellor of Justice Act s. 11^1 (6) states explicit limits to the mandate of the Chancellor of Justice in verifying the intelligence sharing activities – he or she has access to the joint international operations of security authorities or information forwarded by foreign states or international organisations only if the person who forwarded the information has granted consent for access. As receiving the consent requires a number of complicated procedures, the Chancellor of Justice has so far not carried out any checks in this field. Also, considering this restriction, neither the government nor the intelligence agencies are required to inform the Chancellor of Justice about intelligence sharing arrangements they have made with other governments.

Furthermore, the law empowers the Chancellor of Justice to check activities of the executive authorities of Estonia, and not of foreign authorities. Still, the Chancellor of Justice has access to such information if an Estonian security authority (e.g. Estonian Internal Security Service or Estonian Foreign Intelligence Service) has collected the information and transferred it to a foreign state, and if restrictions stated in the Chancellor of Justice Act s. 11^1 (6) are not

Office of the Chancellor of Justice
Kohtu 8, 15193 Tallinn, ESTONIA. Phone: +372 693 8404. Fax: +372 693 8401. info@oiguskantsler.ee www.oiguskantsler.ee

applicable. The Security Authorities Surveillance Select Committee of the Riigikogu does not have such restrictions and have therefore broader monitoring options in this regard.

As a rule, the Chancellor of Justice has access to information gathered by surveillance agencies under the Code of Criminal Procedure, including when operations are carried out in cooperation with foreign countries. Even if the Estonian agencies carry out covert operations at the request of a foreign service and in the context of their criminal case (and later transfer the information to the foreign state), the surveillance files are preserved and can be checked by the Chancellor of Justice.

Please also see the annual reports 2016 and 2017 of the Chancellor of Justice in Estonian and in English for additional information.

Sincerely yours,



Ülle Madise

Heili Sepp +372 693 8419
heili.sepp@oiguskantsler.ee

Odyn Vosman +372 693 8422
odyn.vosman@oiguskantsler.ee

Kertti Pilvik +372 693 8434
kertti.pilvik@oiguskantsler.ee

REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Mr Kari Käsper
Executive Director
Estonian Human Rights Centre

Dr. Gus Hosein
Executive Director
Privacy International
edin@privacyinternational.org
scarlet@privacyinternational.org

Your: 14.09.2017

Our: 27.10.2017, no 2.1.-5/17/1888

Answer to request

As a reply to your letter concerning oversight of intelligence sharing.

Estonian DPA has competence in areas of national security and defence – except the intelligence sharing activities, since according to the Estonian law intelligence information are treated as state secret/ classified information.

However, this exception cannot applied in supervisory activities concerning Schengen and Europol information (see Personal Data Protection Act § 2 (3) - https://www.riigiteataja.ee/en/eli/507032016001/consolide).

Respectfully

[redacted]
authorised by Director General
Estonian DPA

Väike-Ameerika 19 / 10129 Tallinn / 627 4135 / info@aki.ee / www.aki.ee
Registrikood 70004235

OFFICE OF THE PARLIAMENTARY OMBUDSMAN OF FINLAND

REPLY 1 / 1

27.10.2017 EOAK/5559/2017

Privacy International
Gus Hosein

Reference: 18.9.2017 arrived letter

With regard to you questionnaire, on behalf of the Parliamentary Ombudsman Petri Jääskeläinen, I kindly inform you the following.

1. The government or the public authorities concerned are not obliged spontaneously to inform the Parliamentary Ombudsman about intelligence sharing arrangements they have made with other governments.
2. According to the Finnish Constitution (Section 111) the Ombudsman have the right to receive from public authorities or others performing public duties the information needed for their supervision of legality. This means that if the Ombudsman focuses his or her supervision on the co-operation of public authorities with foreign authorities, he or she has access in full all relevant information about the intelligence sharing activities.
3. As mentioned above, yes.
4. The Ombudsman does not have power to review decisions to share intelligence but can undertake independent investigations concerning the intelligence sharing activities of government.
5. No.

[redacted]

FI-00102 Eduskunta, Finland TEL. +358 9 4321 ombudsman@parliament.fi www.ombudsman.fi/english

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION NATIONALE DE CONTRÔLE DES TECHNIQUES DE RENSEIGNEMENT

LE PRÉSIDENT

Paris, le 13 novembre 2017
n°193/CNCTR/2017

Objet : Contrôle du partage de renseignements entre le gouvernement français et des gouvernements étrangers

Référence : Votre courrier du 14 septembre 2017

Messieurs,

Par le courrier mentionné en référence, vous avez adressé à la Commission nationale de contrôle des techniques de renseignement (CNCTR) une note relative aux conséquences sur l'exercice des droits de l'homme du partage de renseignements entre gouvernements. Vous avez en outre saisi la commission de questions portant sur le contrôle exercé par la CNCTR sur l'échange de renseignements entre le gouvernement français et des gouvernements étrangers.

En réponse, je souhaiterais tout d'abord vous présenter le cadre juridique qui régit le contrôle des activités des services de renseignement français par la CNCTR.

La loi du 24 juillet 2015 relative au renseignement, dont les dispositions ont été codifiées au livre VIII du code de la sécurité intérieure, a fixé les conditions de mise en œuvre des techniques de renseignement sur le territoire national avec le souci de renforcer la protection des libertés individuelles. La loi du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, également codifiée, prévoit également une procédure de contrôle par la CNCTR.

La CNCTR a pour mission de s'assurer que les éventuelles atteintes portées à la vie privée par la mise en œuvre de techniques de renseignement soient proportionnées à la gravité des menaces ou au caractère fondamental des enjeux invoqués par les services de renseignement.

MM. Gus HOSEIN, [redacted]
s/c Privacy International
62 Britton street
London
EC1M5UY
United Kingdom

35 rue Saint-Dominique 75700 Paris – Tél. : 01 42 75 69 31 – secretariat@cnctr.fr

Cette mission s'exerce notamment sous la forme d'un contrôle *a priori*, qui consiste à examiner la légalité, ce qui inclut la proportionnalité, de toutes les demandes tendant à la mise en œuvre de techniques de renseignement, notamment au regard des critères énoncés à l'article L. 801-1 du code de la sécurité intérieure. Les demandes sont ensuite soumises, accompagnées de cet avis, au Premier ministre, qui statue.

Le contrôle de la CNCTR porte également, *a posteriori*, sur l'exécution des techniques autorisées par le Premier ministre. La commission veille ainsi à ce qu'aucune technique ne soit mise en œuvre sans autorisation et à ce que les autorisations accordées soient exécutées conformément aux dispositions de la loi. À cette fin, la CNCTR, dont les membres et agents sont habilités au secret de la défense nationale, dispose d'un accès permanent, complet, direct et, pour certaines techniques, immédiat aux relevés de mise en œuvre, aux registres prévus par la loi, aux renseignements collectés ainsi qu'aux transcriptions et extractions effectuées par les services de renseignement. Elle accède également aux dispositifs de traçabilité des renseignements collectés ainsi qu'aux locaux dans lesquels ceux-ci sont conservés.

Les prérogatives de la CNCTR sont renforcées par la faculté d'adresser des recommandations aux services de renseignement, à leur ministre de tutelle ainsi qu'au Premier ministre, lorsque la mise en œuvre d'une technique de renseignement lui paraît entachée d'illégalité ou ne lui paraît plus justifiée au regard des prescriptions légales qui l'ont fondée. Dans ce cas, la commission peut recommander l'interruption de la technique et la destruction des informations collectées.

Si le Premier ministre ne donne pas suite aux avis ou aux recommandations de la CNCTR ou si les suites données sont estimées insuffisantes, la commission peut former un recours devant une formation juridictionnelle spécialisée du Conseil d'État, juge administratif suprême auquel ne peut, en la matière, être opposé le secret de la défense nationale.

S'agissant en particulier des échanges de renseignements entre le gouvernement français et des gouvernements étrangers, je vous indique que la loi n'a pas expressément confié à la CNCTR de pouvoirs de contrôle dans ce domaine ni fait explicitement obligation au gouvernement français d'informer la commission en cas d'échanges.

L'article L. 833-1 du code de la sécurité intérieure définit la mission de la CNCTR en prévoyant qu'elle « *veille à ce que les techniques de recueil de renseignement soient mises en œuvre sur le territoire national* » conformément au cadre légal.

Par ailleurs, le 4° de l'article L. 833-2 du même code ne permet pas, à ce jour, à la CNCTR de demander un accès aux informations que les services de renseignement français pourraient obtenir de leurs homologues. Aux termes de ces dispositions, la commission « *peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de sa mission (...) à l'exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux ou qui pourraient donner connaissance à la commission, directement ou indirectement, de l'identité des sources des services spécialisés de renseignement* ».

35 rue Saint-Dominique 75700 Paris – Tél. : 01 42 75 69 31 – secretariat@cnctr.fr

En revanche, la loi n'interdit pas au gouvernement français de donner, de sa propre initiative, à la commission accès à des informations obtenues de services de renseignement étrangers.

Je vous prie, messieurs, de bien vouloir agréer l'expression de ma considération distinguée.

Francis DELON

35 rue Saint-Dominique 75700 Paris – Tél. : 01 42 75 69 31 – secretariat@cnctr.fr

From: BGH-Pressestelle <Pressestelle@bgh.bund.de>
Subject: WG: Privacy International and Reporters without Borders Germany letter and briefing on oversight of intelligence sharing
Date: 15 September 2017 at 09:04:03 BST
To: "'tomasof@privacyinternational.org'" <tomasof@privacyinternational.org>

Sehr geehrter Herr Dr. Hosein, sehr geehrter Herr Mihr,

vielen Dank für Ihre freundliche Anfrage vom 13. September 2017.

Die Aufgaben, Befugnisse und Zuständigkeiten des Unabhängigen Gremiums (§ 16 BNDG) sind gesetzlich geregelt. Sie können diese dem Gesetz über den Bundesnachrichtendienst (BNDG) entnehmen.

https://www.gesetze-im-internet.de/bndg/BNDG.pdf

Mit freundlichen Grüßen

Dietlind Weinland
Richterin am Bundesgerichtshof
Pressesprecherin

Bundesgerichtshof
-Pressestelle-
pressestelle@bgh.bund.de
Angela Haasters
Herrenstraße 45a
76133 Karlsruhe
Tel.Nr. 0721-159-5013
Fax.Nr. 0721-159-5501

Deutscher Bundestag
G 10-Kommission
Geschäftsstelle

Reporter ohne Grenzen
Friedrichstraße 231
10969 Berlin

Berlin, 4. Oktober 20174. Oktober 2017
Geschäftszeichen:
PK 4-5/2017
Bezug: Ihr Schreiben vom
13. September 2017
Anlagen: 2

Leiter
Referat PK 4
Strukturelle und Ad-hoc-Kontrollen technische Fähigkeiten der Dienste, G10-Angelegenheiten

Platz der Republik 1
11011 Berlin
Telefon: +49 30 227-31300
Fax: +49 30 227-30252
vorzimmer.pk4@bundestag.de

Ihre Zuschrift an den Vorsitzenden der G 10-Kommission

Sehr geehrte Damen und Herren,

Sie haben sich mit Fragen zur internationalen Zusammenarbeit der deutschen mit ausländischen Nachrichtendiensten an den Vorsitzenden der G 10-Kommission, Herrn Andreas Schmidt, gewandt. Der Vorsitzende hat mich gebeten, Ihnen als Leiter der Geschäftsstelle der G 10-Kommission zu antworten.

Lassen Sie mich zunächst darauf hinweisen, dass die Bundesregierung hinsichtlich der Tätigkeit der deutschen Nachrichtendienste grundsätzlich der Kontrolle durch das Parlamentarische Kontrollgremium des Deutschen Bundestages (PKGr) unterliegt. Das Gesetz über das Parlamentarische Kontrollgremium (PKGrG) regelt dessen weitgehende Aufgaben und Befugnisse. Sollten Sie hierzu weitere Fragen haben, rege ich an, dass Sie sich gesondert an den Vorsitzenden des PKGr wenden.

Die G 10-Kommission ist allein für den speziellen Bereich der nachrichtendienstlichen Tätigkeit zuständig, bei dem es um die Überwachung und Aufzeichnung von Telekommunikation unter Beteiligung deutscher Grundrechtsträger oder in Deutschland aufhältiger natürlicher oder juristischer Personen sowie um die Öffnung und Einsicht in Sendungen, die dem Brief- oder Postgeheimnis unterliegen, geht.

Derartige Maßnahmen der Nachrichtendienste, die in Artikel 10 des Grundgesetzes (Brief-, Post- und Fernmeldegeheimnis) eingreifen, bedürfen der Zustimmung der G 10-Kommission (§ 15 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses – Artikel 10-Gesetz - G 10). Die Mitglieder der G 10-Kommission werden vom PKGr gewählt. Sie sind ehrenamtlich tätig, in ihrer Amtsführung unabhängig und Weisungen nicht unterworfen.

Die Kontrollbefugnis der G 10-Kommission erstreckt sich auf die Erhebung, Verarbeitung und Nutzung der durch die o.g. Maßnahmen erlangten personenbezogenen Daten (§ 15 Abs. 5 S. 2 G 10). Der Kommission und ihren Mitarbeiterinnen und Mitarbeitern ist dabei von den Nachrichtendiensten insbesondere (1.) Auskunft zu ihren Fragen zu erteilen, (2.) Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Beschränkungsmaßnahme stehen, und (3.) jederzeit Zutritt in alle Diensträume zu gewähren (§ 15 Abs. 5 S. 2 G 10).

Von der Kontrollbefugnis der Kommission umfasst ist somit auch die Übermittlung von Daten an ausländische Nachrichtendienste, soweit diese durch Maßnahmen gewonnen wurden, die der Zustimmung der G 10-Kommission bedürfen.

Zu Ihrer Information übermittle ich Ihnen in der Anlage die Texte des PKGrG und des G10.

Ich hoffe, ihnen mit diesen Hinweisen und Unterlagen weitergeholfen zu haben und verbleibe

mit freundlichen Grüßen

[redacted]

Nemzeti Adatvédelmi és
Információszabadság Hatóság

Ügyszám: NAIH/2017/4694/2/T.

Majtényi László DSc.
Eötvös Károly Intézet
elnök

és

Dr. Gus Hosein
Privacy International

részére

tomasof@privacyinternational.org

Tisztelt Dr. Gus Hosein Úr és tisztelt Majtényi László Úr!

A Nemzeti Adatvédelmi és Információszabadság Hatósághoz (továbbiakban: Hatóság) 2017. szeptember 14-én érkezett beadványukban tájékoztatást kérték a magyar kormányzat, illetve a nemzetbiztonsági szolgálatok és a külföldi kormányok között létrejött információcserével kapcsolatos megállapodások átláthatósága tárgyában.

A levelükben feltett kérdésekre a következő válaszokat adom.

K1. „A kormány és/vagy a hírszerző ügynökségek kötelesek-e tájékoztatni Önt olyan információcserére vonatkozó megállapodásokról, amelyeket más kormányokkal kötöttek?"

V.: A Hatóság feladatait és hatáskörét az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) határozza meg. Az Infotv. 38. § (2) bekezdése szerint a Hatóság feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése. Az Infotv. 38. § (4) bekezdés a) pontja értelmében a Hatóság a (2) bekezdés szerinti feladatkörében javaslatot tehet a személyes adatok kezelését, valamint a közérdekű adatok és a közérdekből nyilvános adatok megismerését érintő jogszabályok megalkotására, illetve módosítására, véleményezi a feladatkörét érintő jogszabályok tervezetét. Ennek értelmében a Hatóság előzetesen, a jogszabály-előkészítés folyamatában értesül azokról a két- és többoldalú, nemzetbiztonsági célú adatátadást érintő egyezményekről és megállapodásokról, amelyeket a magyar jog szerint jogszabályban kell kihirdetni.

Ezen túlmenően a hazai és uniós jogszabályok előírásai alapján a nemzetbiztonsági szolgálatoknak nincs tájékoztatási vagy bejelentési köztelezettségük az együttműködéseik konkrét részleteit illetően.

1125 Budapest,
Szilágyi Erzsébet fasor 22/C.

Tel.: +36 1 391-1400
Fax: +36 1 391-1410

ugyfelszolgalat@naih.hu
www.naih.hu

K2.: „Az Ön feladata magában foglalja a kormány által végzett hírszerzési információk megosztásának független felügyeletét?"

V.: Az Infotv. hatálya a Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik (a természetes személyek kizárólag saját személyes céljait szolgáló adatkezeléseit kivéve.). A Hatóság ellenőrzési feladat- és hatásköre valamennyi, az Infotv. hatálya alá tartozó adatkezelésre kiterjed, beleértve a nemzetbiztonásgi szolgálatok által végzett adatkezelést is.

K3.: „Rendelkezik-e olyan jogosítványokkal, hogy teljes mértékben hozzáférhessen a hírszerzéssel kapcsolatos kormányzati tevékenységet érintő összes lényeges információhoz?"

V.: Az Infotv. 71. § (1) bekezdése szerint a Hatóság eljárása során - az annak lefolytatásához szükséges mértékben és ideig - kezelheti mindazon személyes adatokat, valamint törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatokat, amelyek az eljárással összefüggnek, illetve amelyek kezelése az eljárás eredményes lefolytatása érdekében szükséges. Az Infotv. 71. § (4) bekezdése szerint a minősített adatot érintő adatkezeléssel kapcsolatos eljárása során a Hatóság elnökhelyettese, vezetői munkakört betöltő köztisztviselője és vizsgálója - ha megfelelő szintű személyi biztonsági tanúsítvánnyal rendelkezik - a minősített adatot a minősített adat védelméről szóló törvényben meghatározott felhasználói engedély nélkül is megismerheti.

Az Infotv. 71. § (3) bekezdése az alapvető jogok biztosáról szóló 2011. évi CXI. törvényre utalva a következő adatok és adatforrások megismerését korlátozza a Hatóság nemzetbiztonsági szolgálatokat érintő eljárásai során:

a) a nemzetbiztonsági szolgálatokkal együttműködő magánszemélyek azonosítására szolgáló nyilvántartás,
b) a nemzetbiztonsági szolgálatok által titkos információgyűjtésre használt eszközök és módszerek működésének és működtetésének műszaki-technikai adatait tartalmazó vagy az azokat alkalmazó személyek azonosítását lehetővé tevő irat,
c) a rejtjeltevékenységgel és kódolással kapcsolatos irat,
d) a nemzetbiztonsági szolgálatok objektumaival és állományával kapcsolatos biztonsági dokumentumok,
e) a biztonsági okmányvédelemmel és technológiai ellenőrzéssel kapcsolatos irat,
f) olyan iratba, amelynek megismerése az információforrás azonosítását lehetővé tenné, valamint
g) olyan irat, amelynek megismerése a nemzetbiztonsági szolgálatok külföldi partnerszolgálatok irányában vállalt kötelezettségeit sértené.

A fentiek közül a g) pontban írt korlátozás érintheti a nemzetbiztonsági szolgálatok által kezelt adatok külföldre továbbításának ellenőrzését.

Megemlítem, hogy a fenti korlátozások nem azt jelentik, hogy a fenti adatkezelések egyáltalán nem ellenőrizhetők a Hatóság által, hanem azt, hogy ezekben az esetekben az alapvető jogok biztosáról szóló törvény 23. § (7) bekezdése szerinti eljárásrendet kell alkalmaznunk, vagyis ha a Hatóság az ügy teljes körű feltárása érdekében a fentebb felsoroltak körébe tartozó iratok megvizsgálását is szükségesnek tartja, a feladatkörrel

rendelkező minisztertől kérheti azok megvizsgálását. A feladatkörrel rendelkező miniszter köteles a Hatóság által megkívánt vizsgálatot elvégezni vagy elvégeztetni, és a vizsgálat eredményéről a Hatóságot az általa megállapított határidőn belül tájékoztatni. A határidő nem lehet rövidebb harminc napnál.

K4.: „Megvan az a hatásköre, hogy felülvizsgálja az információ-megosztással kapcsolatos kormányzati döntéseket, vagy Önálló vizsgálatokat folytasson e tekintetben?"

V.: A Hatóság az Infotv.-ben meghatározottak szerint vizsgálati eljárást, adatvédelmi eljárást és titokfelügyeleti hatósági eljárást folytathat a nemzetbiztonsági szolgálatok adatkezelésével kapcsolatban. (A titokfelügyeleti hatósági eljárás során csak a nemzeti minősített adatok minősítésének jogszerűsége vizsgálható, a külföldi minősített adatoké nem).

Ami az információ-megosztással kapcsolatos kormányzati döntések ellenőrzését illeti az 1. kérdésre adott válaszban említett egyeztetés során a Hatóság véleményezési jogkörrel rendelkezik.

K5.: „Együttműködik más, hazai vagy külföldi felügyeleti testületekkel annak értekében, hogy ellenőrizze a kormányzat hírszerző, információt megosztó tevékenységét?"

V.: A Hatóság együttműködik az uniós társhatóságokkal, illetve egyedi ügyekben más unión kívüli adatvédelmi hatóságokkal is az adatvédelem területén. A Privacy Shield mechanizmus keretében veszünk részt kormányzati hírszerző, információ megosztó tevékenységek ellenőrzésében.

Budapest, 2017. november „ 10 „.

Üdvözlettel:

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG 1. SZ.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár

This document is an unofficial translation by Privacy International of the original text.

National Data Protection and
Information Freedom Authority

Document Number: NAIH/2017/4694/2/T.

DSc. Majtenyi Laszlo
Eötvös Károly Institute
President

And

Dr. Gus Hosein
Privacy International

for

tomasof@privacyintemational.org

Dear Dr. Gus Hosein and Dear Majtényi László!

In the document sent to National Data Protection and Information Freedom Nationality (furthermore: Authority) on 14 September 2017, you asked for information about the transparency of agreements made between the government of Hungary, the national security services and foreign governments on the exchange of information.

I give the following answer the questions raised in your letter.

K1. "Are the Government and the intelligence agency obliged to inform you about information exchange agreements made with other governments?"

V.: The roles and scope of the power of the Authority are defined in law 2011/112 on Right of Self-declaration and Freedom of Information (furthermore: Infotv.). According to section 38. § (2) of Infotv. the role of the Authority is to support and control the fulfillment of rights related to the protection of personal data, as well as the right to be able to learn about public information and information of public interest. According to section 38. § (4) Article a), the Authority can make a suggestion based on Article (2) to make or amend regulation affecting the handling of personal data, and the publication of public information and information with a public interest, as well as the comment of draft resolutions. This means that the Authority is informed early, during the stage of preparation, about the two- or more sided agreements related to transfer of information related to national security, which, according to Hungarian law, must be published in a decree.

Furthermore, based on the requirements of Hungarian and Community law, the national security services have no reporting obligation related to the details of their cooperation.

1125 Budapest,
Szilágyi Erzsébet fasor 22/C.

Tel.: +36 1 391-1400
Fax: +36 1 391-1410

ugyfelszolgalat@naih.hu
www.naih.hu

K2.: "Does your task involve the independent control of sharing the intelligence information obtained during the activities of the government?"

V.: The scope of effect of Infotv. covers all data handling and data processing activity, which is related to personal data or public data or data of public interest (except the handling of personal information for their own purpose). The control and obligation scope of effect of the Authority includes all data handling under Infotv., including handling of data by the national security services.

K3.: "Do you have licenses which makes it possible to fully access all important information related to national security activities?"

V.: According to the Article. 71. § (1) of Infotv., during the process of the Authority - up to the extent and time needed for its fulfillment - it can handle all the personal information and data needed to handle personal information, which are classified as secret by law, which are related to the process, and which is necessary to successfully carry out the process. According to section 71. § (4) of Infotv., during the process of handling classified information, the Vice president of the Authority, its officers in charge and auditor - when given the necessary level of personal security license - may learn the classified personal data without having the license defined in the law on the protection of classified data.

Section 71. § (3) of Infotv., referring to law 2011/111 on the Committee of basic rights, limits the publication of the following data and data sources during the processes of Authority related to national security services:

a) administration of personnel working with the national security services,
b) document defining the tools and methods used for secret collection of information, the technical details of operation and workings, and the identification of personnel operating these,
c) document related to coding and decoding,
d) security documents related to national security documents and personnel,
e) document related to security document protection and technological verification,
f) a document making the identification of the source of information possible,
g) a document which would harmfully effect the obligations of national security services towards foreign partner organizations,

From the above, the limitation defined in section g) may have an effect on the transfer of information of data handled by the national security services.

I would like to mention that limitations do not mean that the information handling mentioned above cannot be controlled by the Authority, but that we need to use the process defined in Article 23. § (7) on the Committees of Basic rights, so when the Authority considers it important to check any of the documents belonging to the classification mentioned earlier, the Minister in this role might be requested to verify these. The Minister in this role is obliged to perform or have performed the control requested by the Authority, and to inform the Authority about the result of verification within the deadline defined by him. The deadline cannot be shorter than thirty days.

K4.: "Do you have the power to supervise the government decisions related to sharing of information, or to perform independent examinations with this regard?"

V.: The Authority can perform a verification process, data protection process and formal secrecy control process related to the data processing of national security services. (During the secret handling process, only the legibility of national data classification can be examined, and not of foreign classified information).

Related to the verification of government decrees associated with sharing of information, for the control defined in the first answer given, the Authority has a right for commenting.

K5.: "Do you cooperate with other national or foreign controlling bodies in order to control the intelligence and information sharing activity of the government?"

V.: The Authority cooperated with similar bodies of the EU, and in individual cases, with other data protection authorities in the field of data protection. Within the framework of Privacy Shield mechanism, we take part in the control of national intelligence and national sharing activities.

Budapest, 10 November 2017

Sincerely

[Stamp]
[Signature]
Dr. Péter Vitál
President
university teacher

From: **INFO** info@justice.ie
Subject: Response
Date: 4 April 2018 at 16:00
To: scarlet@privacyinternational.org

scarlet@privacyinternational.org

4 April 2018

Our Ref: MIN/2017/470

Dear Dr Hosein, Dr McIntyre, and Mr Herrick,

I am directed by the Minister for Justice and Equality, Mr Charlie Flanagan, T.D., to refer to your correspondence regarding oversight of intelligence sharing between Ireland and foreign governments. The delay in replying is regretted.

The policing powers and duties of members of An Garda Síochána are set out in the Garda Síochána Acts 2005-2015, including that the direction and control of An Garda Síochána are matters for the Garda Commissioner. Those Acts set out also the mechanisms for oversight of policing services by the Policing Authority and for the investigation of complaints about Garda conduct by the Garda Síochána Ombudsman Commission. Members of An Garda Síochána are subject not just to the provisions of the Garda Síochána Acts but to the law generally and also to the Garda codes and regulations in carrying out their duties, including the Code of Ethics published by the Policing Authority in January 2017.

Section 28 of the Garda Síochána Acts 2005-2015 allows for the Garda Commissioner, with the consent of the Government to enter into agreements with police forces or law enforcement agencies outside the State for a range of purposes.

For security reasons, it is not the practice to publicly comment on the detail of counter-terrorism arrangements. It should be noted that our history on this island means that regrettably we have been engaged in counter-terrorism work for decades and the arrangements currently in place have served the Irish people well in countering threats to the security of the State. The Gardaí and Defence Forces have a long and proud record in protecting and defending the State from a sustained terrorist threat over many years.

That said, given the dynamic and evolving nature of security threats, particularly from international terrorism, these arrangements are kept constantly under review, including the decision-making arrangements across the common areas of the State's security and defence.

You will no doubt be aware that the Commission on the Future of Policing in Ireland, which is comprised of national and international experts, is currently undertaking a comprehensive examination of all aspects of policing in the state, including the appropriate structures for governance, oversight and accountability, and the legislative framework for policing to ensure that it is adequate to meet the challenges of modern policing. The Commission has undertaken a wide ranging consultation and the Minister would encourage you to engage with them if you have not already done so. The Commission is to report by September 2018 and will, on the basis of its findings, bring forward proposals for the future of policing, including appropriate recommendations for legislative change. The Minister looks forward to the receipt of these proposals which will be given full consideration by the Government.

Yours sincerely

From: **Bos-Ollermann, H.T.** H.Bos-Ollermann@CTIVD.nl
Subject: Questions regarding oversight of intelligence sharing
Date: 19 September 2017 at 06:33
To: scarlet@privacyinternational.org
Cc: [redacted]

HB

Dear mr Hosein, dear ms Kim,

Last week [redacted] forwarded your letter to Harm Brouwer about oversight of intelligence sharing.

Of course we are willing to respond to your questions, you will find our answers below.

- *Is the government and/or are the intelligence agencies required to inform you about intelligence sharing arrangements they have made with other governments?*

Yes. The intelligence agencies are by law (article 73, Intelligence and Security Services Act 2002) obliged to furnish all information the Review Committee on the Intelligence and Security Services (abbreviated in Dutch: CTIVD) deems necessary for a proper performance of its duties. The CTIVD is also given the right to immediate access to all information. In practice, our investigators can access any processed data directly, including intelligence sharing arrangements.

- *Does your mandate include independent oversight of the intelligence sharing activities of your government?*

Yes. The CTIVD has the task to oversee the legitimacy of the activities of the Dutch intelligence and security services. This includes the intelligence sharing with services of other countries.

- *Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?*

Yes, see above.

- *Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government?*

Yes, see above.
To give some examples, I would like to refer you a few recent public Review Reports that are translated into English. These reports deal with different aspects of international cooperation between intelligence and security services, with a strong focus on intelligence sharing:

  - Review Report 48 on the implementation of cooperation criteria by the AIVD and the MIVD (https://english.ctivd.nl/investigations/r/review-report-48)
  - Review Report 49 on the exchange of unevaluated data by the AIVD and the MIVD (https://english.ctivd.nl/investigations/r/review-report-49)
  - Review Report 50 on contributions of the MIVD to targeting (https://english.ctivd.nl/investigations/r/review-report-50)

- *Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the*

intelligence sharing activities of your government?

Yes. We started a joint project on this topic in 2015. You will find information about this in chapter 7 of our annual report 2016 (https://english.ctivd.nl/latest/news/2017/07/24/index) and in chapter 7 of our annual report 2015 (https://english.ctivd.nl/publications/documents/annual-reports/2016/06/07/annual-report-2015)

Do not hesitate to contact me should you have any further questions.

Kind regards,

Hilde Bos-Ollermann
General Secretary CTIVD

T: 00 31 70 - 3155820 | M: 00 31 6 - 51261539
www.ctivd.nl

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

18 September 2017

Dr. Gus Hosein and David Tong
Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

By Email: scarlet@privacyinternational.org

Dear Dr Hosein and Mr Tong

Thank you for your letter of 13 September 2017.

Your briefing *Human Rights Implications of Intelligence Sharing* raises important issues which we grapple with in the context of my office's oversight of the legality and propriety of the activities of New Zealand's intelligence and security agencies.

I am currently conducting a (publicly announced) inquiry into whether the New Zealand agencies had knowledge of or involvement in the CIA detention and interrogation programme of 2001/09, as set out in the US Senate Intelligence Committee report of December 2014. A significant part of my inquiry is focused on what safeguards the agencies had at that time, and have now, to avoid the possibility of being implicated in unlawful activity by their foreign counterparts. This necessarily involves looking at current and past intelligence sharing practices. I will report publicly at the conclusion of my inquiry which is still some months away.

In the meantime I am happy to provide answers to the questions set out in your letter, to the extent I can, and will endeavour to do that by 31 October 2017 as you request.

Yours sincerely

Cheryl Gwyn
Inspector-General of Intelligence and Security

P O Box 5609, Wellington 6140
enquiries@igis.govt.nz
Phone: 04 471 8683

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

27 October 2017

Dr. Gus Hosein and David Tong
Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

By email: scarlet@privacyinternational.org

Dear Dr Hosein and Mr Tong

I write in response to your letter of 13 September 2017. I value Privacy International's focus on the role of oversight bodies, as one means by which the lawfulness and propriety of actions of intelligence and security agencies receive scrutiny and review. Alongside the work of other official oversight bodies, civil society organisations such as Privacy International help ensure the transparency of those activities, and also of course serve to 'watch the watchers' which is enormously valuable in an open democracy. As your briefing canvassed, information sharing is a key function of intelligence and security agencies, with the agencies accountable for the extent to which those arrangements comply with international and domestic human rights law.

By way of introduction, I provide a few notes on the role of the Inspector-General of Intelligence and Security, and the current framework, both statutory and organisational, for intelligence and security agencies in New Zealand.

Inspector-General of Intelligence and Security

The office of the Inspector-General of Intelligence and Security (Inspector-General) in New Zealand is independent of the executive. The Inspector-General has oversight of the two intelligence and security agencies, the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS).

In summary, my office has the functions, duties and powers to:

- ensure the intelligence and security agencies conduct their activities lawfully and with propriety
- ensure that complaints relating to the intelligence and security agencies are independently investigated, and

P O Box 5609, Wellington 6140
enquiries@igis.govt.nz
Phone: 04 817 0402

- advise the New Zealand Government and Intelligence and Security Committee on matters relating to the oversight of the agencies.[1]

To fulfil these responsibilities I have jurisdiction to:

- receive complaints
- initiate inquiries into the legality and/or propriety of agency activities
- review the agencies' internal operational systems, and
- review all intelligence warrants.

My office is also able to receive and, where appropriate, investigate protected disclosures (aka whistleblowing) relating to classified information and/or the activities of the intelligence and security agencies.[2] Information about my role, functions and the work undertaken by my office is available in our Annual Reports[3] (with some further details provided below).

New Zealand's intelligence community[4]

The intelligence community comprises two civilian intelligence collection agencies:

- the GCSB[5] – primarily focuses on foreign signals intelligence (SIGINT)
- the NZSIS[6] – primarily focuses on domestic human intelligence (HUMINT).

In the New Zealand intelligence community there is also a civilian intelligence analysis and reporting agency, the National Assessments Bureau within the Department of the Prime Minister and Cabinet, and a range of intelligence functions within agencies including Defence, Customs, Immigration and Police. None of these is subject to specialist independent oversight, although they are subject to more general public sector oversight by the Office of the Ombudsmen and the Office of the Privacy Commissioner.

Review of intelligence and security: Intelligence and Security Act 2017

An independent review of intelligence and security in New Zealand, in February 2016, recommended a complete overhaul of the statutes governing the GCSB, NZSIS and their oversight. The recommendations, set out in the Report *Intelligence and Security in a Free Society*,[7] are now largely implemented by the Intelligence and Security Act 2017 (IS Act), which came into effect on 28 September 2017.

Acting in compliance with human rights law

In keeping with the review's recommendations, the IS Act includes requirements that the GCSB and NZSIS "act in accordance with New Zealand law and all human rights obligations recognised by New

[1] Intelligence and Security Act 2017 (IS Act), ss 156, 158 and 171. All New Zealand legislation is available at www.legislation.govt.nz
[2] Protected Disclosures Act 2000, ss 12 and 13; IS Act, s 160.
[3] Inspector-General of Intelligence and Security Annual Reports are available at www.igis.govt.nz/publications/annual-reports/
[4] NZIC website is available at www.nzic.govt.nz
[5] GCSB website is available at www.gcsb.govt.nz
[6] NZSIS website is available at www.nzsis.govt.nz
[7] Sir Michael Cullen and Dame Patsy Reddy *Intelligence and Security in a Free Society* February 2016, available via search at www.parliament.nz/

Zealand law".[8] Of particular relevance to Privacy International's enquiry are sections 10 and 12 of the IS Act which require the responsible Minister to be "satisfied" of this compliance, before authorising the agencies to share information with overseas public authorities / foreign parties and undertake foreign cooperation.

Ministerial Policy Statements under the new Act

The IS Act also requires the Minister responsible for the NZSIS and GCSB to issue Ministerial Policy Statements (MPSs), to provide guidance for the agencies on the conduct of lawful activities in 13 areas.[9] The Office of the Inspector-General was consulted during the development of these MPSs. Of particular relevance to intelligence sharing is the MPS entitled *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities*.[10] I comment further on this specific MPS below.

Responses to Privacy International's questions

1. Is the government and/or are the intelligence agencies required to inform you about intelligence sharing arrangements they have made with other governments?

There is no legislative provision requiring the GCSB or NZSIS (or any other government body) to proactively inform the Inspector-General about current or new intelligence sharing arrangements with other governments or foreign agencies. It is a matter of public record that New Zealand's primary intelligence sharing relationships are with New Zealand's Five Eyes partners of USA, UK, Australia and Canada.

However, the IS Act requires that, where the GCSB or the NZSIS request a government of, or an entity in, another jurisdiction to carry out an activity that would be an unlawful activity if it were carried out by the GCSB or NZSIS, they must obtain an intelligence warrant. As my office reviews all intelligence warrants, any such request and associated intelligence cooperation agreements will be subject to my oversight.[11]

More generally, in order to carry out the Inspector-General's functions and duties, I have broad rights of access to all agency information which can, as necessary, include access to NZSIS or GCSB's intelligence sharing arrangements with other countries and foreign agencies. (These powers are noted below in response to your third question).

2. Does your mandate include independent oversight of the intelligence sharing activities of your government?

Yes, to the extent that my mandate includes independent oversight of the intelligence sharing activities of New Zealand's two intelligence and security agencies, the GCSB and NZSIS, both of which are government departments.

---

[8] IS Act, ss 3(c), 10(3), 12(7), 17(a) and 18(b).
[9] IS Act, ss 206, 207 and 209.
[10] The MPSs are available at www.nzic.govt.nz/legislation/
[11] IS Act, s 49(2).

Key points to note are:

- My office is independent of the agencies themselves and executive government. Key features of this independent status are that my office is funded by an appropriation that sits outside of the intelligence community; the appointments of the Inspector-General and Deputy Inspector-General are made without reference to the agencies; these roles are both independent statutory officers, not employees; I am not subject to direction from the Prime Minister or any Minister in terms of how I carry out my role
- The IS Act provides for total, unmediated access to security information held by the intelligence and security agencies
- I can initiate an inquiry into the lawfulness and propriety of agency activities, where that is in the public interest and without the need for government request or concurrence, and
- The IS Act requires that I report publicly, annually and on specific inquiries. This is an important aspect of my independence and of transparent and effective oversight and public accountability.

My office is small (eight people in total) which requires us to carefully prioritise where we put out resources and our focus in terms of overseeing all of the agencies' activities. That said, I am satisfied that as a team we do manage to achieve sufficiently broad and also in-depth coverage. My work programme and Annual Report are published each year, and also tabled in the House, which allows the public to form its own view of the effectiveness and productivity of this office.

3. Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?

Yes, as noted above, I have broad rights of access to agency information as necessary to carry out all my statutory functions and duties. In addition, in the context of an inquiry the IS Act provides the Inspector-General with powers to:

- require any person to provide any information, document or thing in that person's possession or control, that I consider relevant to an inquiry[12]
- receive in evidence any statement, document, information or matter that may assist me with an inquiry, whether or not that material would be admissible in a court of law[13]
- require disclosure to the Inspector-General of any matter, despite that information, document, thing or evidence being subject to an obligation of secrecy under an enactment or otherwise[14]
- summons persons I consider able to give information relevant to an inquiry,[15] and
- enter, at a reasonable time, any premises used by an intelligence and security agency.[16]

Any person answering questions, giving evidence or providing information documents or things to the Inspector-General has the same privileges as witnesses have in a court of law.[17]

[12] IS Act, s 179.
[13] IS Act, s 176.
[14] IS Act, s 180.
[15] IS Act, s 178.
[16] IS Act, s 184.
[17] IS Act, s 181.

4. Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government?

Such a review could arise in a number of ways. For example, it can occur in relation to my investigation of a specific complaint received by the Inspector-General, or with regard to regular review of all intelligence warrants. Intelligence sharing activities may be considered as part of an own-motion inquiry.[18]

Inquiry into possible New Zealand engagement with Central Intelligence Agency detention and interrogation 2001-2009

As I mentioned in my interim reply of 18 September 2017, I am currently conducting a (publicly announced) inquiry into whether the New Zealand intelligence and security agencies had knowledge of or involvement in the CIA detention and interrogation programme of 2001- 2009, as set out in the US Senate Intelligence Committee report of December 2014. I expect my inquiry will result in the clarification of past events; it will also include an assessment of whether relevant standards, in policy, procedure and practice, are currently in place.

A significant part of my inquiry is focused on what safeguards the agencies had at that time, and have now, to avoid the possibility of being implicated in unlawful activity by their foreign counterparts (for example, through agency activities that might amount to complicity in acts of torture). This necessarily involves looking at the agencies' past and present intelligence sharing arrangements, policies and practices, alongside New Zealand's obligations under international and domestic human rights law.

Ministerial Policy Statement on co-operation with overseas public authorities

The IS Act[19] requires that, in conducting any inquiry or review, I must take into account any relevant Ministerial Policy Statement (MPS) and the extent to which the agency has had regard to that statement.

The MPS entitled *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities,* has as its primary purpose the provision of "guidance on determining which overseas public authorities GCSB and NZSIS should engage with, and how that engagement should be regulated, including guidance on the types of activities that are appropriate to undertake with those parties".[20] The MPS also "addresses issues associated with the operational use of intelligence gained from a foreign partner".[21]

Parts of the MPS address the use of information by intelligence and security agencies when the information is known or suspected to have been obtained by human rights abuses, such as torture. I

---

[18] IS Act, s 158.
[19] IS Act, s 158(2).
[20] Ministerial Policy Statement *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities*, at [8].
[21] Ministerial Policy Statement *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities*, at [8].

acknowledge that some aspects of the law on complicity in this context have not yet fully crystallised, but I have made the New Zealand agencies aware of my view that these parts of the MPS require further consideration and careful development. Other jurisdictions are also considering this issue - see, for example, the recently redrafted Canadian *Ministerial Directions on Avoiding Complicity in Mistreatment by Foreign Entities*. The MPS itself contemplates a review within a relatively short time.[22]

5. Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government?

Yes, I greatly value the collegial relationships, and discussions on issues (to the extent that our respective laws allow), that my office has with oversight bodies around the world, including bodies in the other Five Eyes countries, and in certain European states with whom I have established relationships.

Broader and deeper international cooperation between intelligence and security agencies represents a growing challenge to accountability. I view this increasing accountability deficit as perhaps the most significant oversight challenge in the field of national security today.

At a domestic level, I may consult with any of the Auditor-General, an Ombudsman, the Privacy Commissioner, Human Rights Commissioner and the Independent Police Conduct Authority, about matters relating to my statutory functions. In doing so I may disclose any information that I consider necessary for the purpose of the consultation, despite the general restriction on the Inspector-General and staff disclosing any security records or other official information about the activities of an intelligence and security agency.[23]

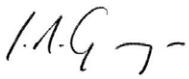
As to international oversight cooperation, to date, national investigations have built on each other, rather than being coordinated across jurisdictions. For example, my work on the 'Inquiry into possible New Zealand engagement with Central Intelligence Agency detention and interrogation 2001-2009' has been assisted by inquiry reports published by oversight bodies in other jurisdictions.

At a recent meeting of the newly established Five Eyes Intelligence Oversight and Review Council, the potential to carry out joint oversight projects was canvassed. I am actively pursuing possibilities for carrying out parallel investigations with foreign oversight bodies to examine specified operational activities or, possibly, both or all "ends" of a particular intelligence agency activity carried out across national borders. Any such investigations or joint projects should result in public reports.

[22] Ministerial Policy Statement *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities*, at [67].
[23] IS Act, s 161.

I hope my responses have addressed all the matters raised by your enquiries. Please do not hesitate to contact my office again with further queries or for any points of clarification. I am also happy to meet in person with the Aotearoa New Zealand Human Rights Lawyers' Association, if that would assist.

Yours sincerely



Cheryl Gwyn
Inspector-General of Intelligence and Security

DEPARTMENT
of the PRIME MINISTER
and CABINET

16 November 2017

Dr Gus Hosein
Privacy International

David Tong
Aotearoa New Zealand Human Rights Lawyers Association

c/o Scarlet Kim (scarlet@privacyinternational.org)

Dear Dr Hosein and Mr Tong

Oversight of intelligence sharing between your government and foreign governments

I write in response to your letter to the Prime Minister and members of the Intelligence and Security Committee of Parliament (the ISC) dated 13 September 2017, about oversight of intelligence sharing between the New Zealand Government and foreign governments. In that letter you asked the ISC a number of questions about oversight of intelligence sharing arrangements in New Zealand.

The ISC is comprised of government and opposition members of the New Zealand House of Representatives. At the time of writing, the ISC does not have any endorsed members following the 2017 General Election and the opening of a new Parliament. This means that the ISC cannot currently conduct any business. In the meantime, the Department of the Prime Minister and Cabinet (DPMC) is able to offer answers to your questions.

DPMC administers the Intelligence and Security Act 2017 (the Act). The Act sets out the functions and powers of the intelligence and security agencies, as well as those relating to the agencies' oversight bodies. In New Zealand, the intelligence and security agencies are the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS).

The Act expressly requires the intelligence and security agencies to act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law when performing their statutory functions. The Act places a duty on the Directors-General of the GCSB and NZSIS to take all reasonable steps to ensure that any cooperation with foreign jurisdictions and international organisations in the performance of any of the agencies' functions is in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

Further, when authorising the sharing of intelligence with any party, foreign or otherwise, the Minister responsible for the intelligence and security agencies must be satisfied that such sharing will be in accordance with those same obligations. The Act also specifies the

Executive Wing, Parliament Buildings, Wellington, New Zealand 6011
☎ 64 4 817 9700 Facsimile 64 4 472 3181 www.dpmc.govt.nz

powers and responsibilities of the Inspector-General of Intelligence and Security (the Inspector-General) as an independent oversight body and the ISC, which exercises oversight on behalf of Parliament.

1. **Is the government and/or are the intelligence agencies required to inform you about intelligence sharing arrangements they have made with other governments?**

You may be interested to know that the Ministerial Policy Statement on the *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities* requires the intelligence and security agencies to refer all new bilateral or multilateral arrangements relating to cooperation and intelligence sharing with a foreign jurisdiction or overseas public authority to the ISC for noting. This ministerial policy statement was issued by the agencies' responsible Minister pursuant to the Act, and must be provided by the Minister to the ISC once it is constituted.[1]

There is no legislative requirement for the intelligence and security agencies to inform the ISC about existing intelligence sharing arrangements.

2. **Does your mandate include independent oversight of the intelligence sharing activities of your government?**

The ISC, as a Parliamentary oversight body, provides democratic oversight of the intelligence and security agencies. Its role is mainly around issues of efficacy and efficiency, budgetary matters, and policy settings.

Independent oversight of the intelligence and security agencies is provided by the Inspector-General. The Inspector-General's oversight function relates to all activities carried out by the intelligence and security agencies in the performance of their statutory functions, including intelligence sharing.

The ISC may request the Inspector-General to undertake an inquiry into an intelligence and security agency's compliance with the law (including human rights law) and the propriety of particular agency activities (conducting such inquiries are functions of the Inspector-General). Where she undertakes an inquiry at the ISC's request, the IGIS must report the results of that inquiry to the ISC. This function gives the ISC a mechanism for ensuring issues of concern to it are independently investigated.

As set out in the Act, the ISC's functions are:

- to examine the policy, administration, and expenditure of each intelligence and security agency;
- to receive and consider the annual report of each intelligence and security agency;
- to conduct each year, following receipt of the annual report of an intelligence and security agency, an annual review of the agency for the immediately preceding financial year;
- to consider any Bill, petition, or other matter in relation to an intelligence and security agency referred to the Committee by the House of Representatives;

[1] Available at https://www.nzic.govt.nz/assets/MPSs/Ministerial-Policy-Statement-Cooperation-with-overseas-public-authorities.pdf.

- to request the Inspector-General to conduct an inquiry into-
    - any matter relating to an intelligence and security agency's compliance with New Zealand law, including human rights law;
    - the propriety of particular activities of an intelligence and security agency;
- to consider any matter (not being a matter relating directly to the activities of an intelligence and security agency) referred to the Committee by the Prime Minister because of that matter's intelligence or security implications;
- to consider and discuss with the Inspector-General his or her annual report.

The ISC's functions do not include inquiring into any matter within the jurisdiction of the Inspector-General, nor the examination of any operational matters.

3. **Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?**

The ISC has the ability to request the Director-General of an intelligence and security agency, or any other person, to disclose any document or other information relevant to the matters being considered by the ISC. That information must be provided unless the circumstances set out in sections 202 and 203 of the Act apply.

The Inspector-General has a very broad right of access to any information held by an intelligence and security agency. The Act also contains provisions applying to the Inspector-General's access to information when conducting an inquiry under the Act (for example, see sections 178 and 180).

4. **Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning intelligence sharing activities of your government?**

This is not a function of the ISC. However, agency decisions relating to intelligence sharing may be something the IGIS examines in the course of investigating a specific complaint or in the course of an own-motion inquiry, for example.

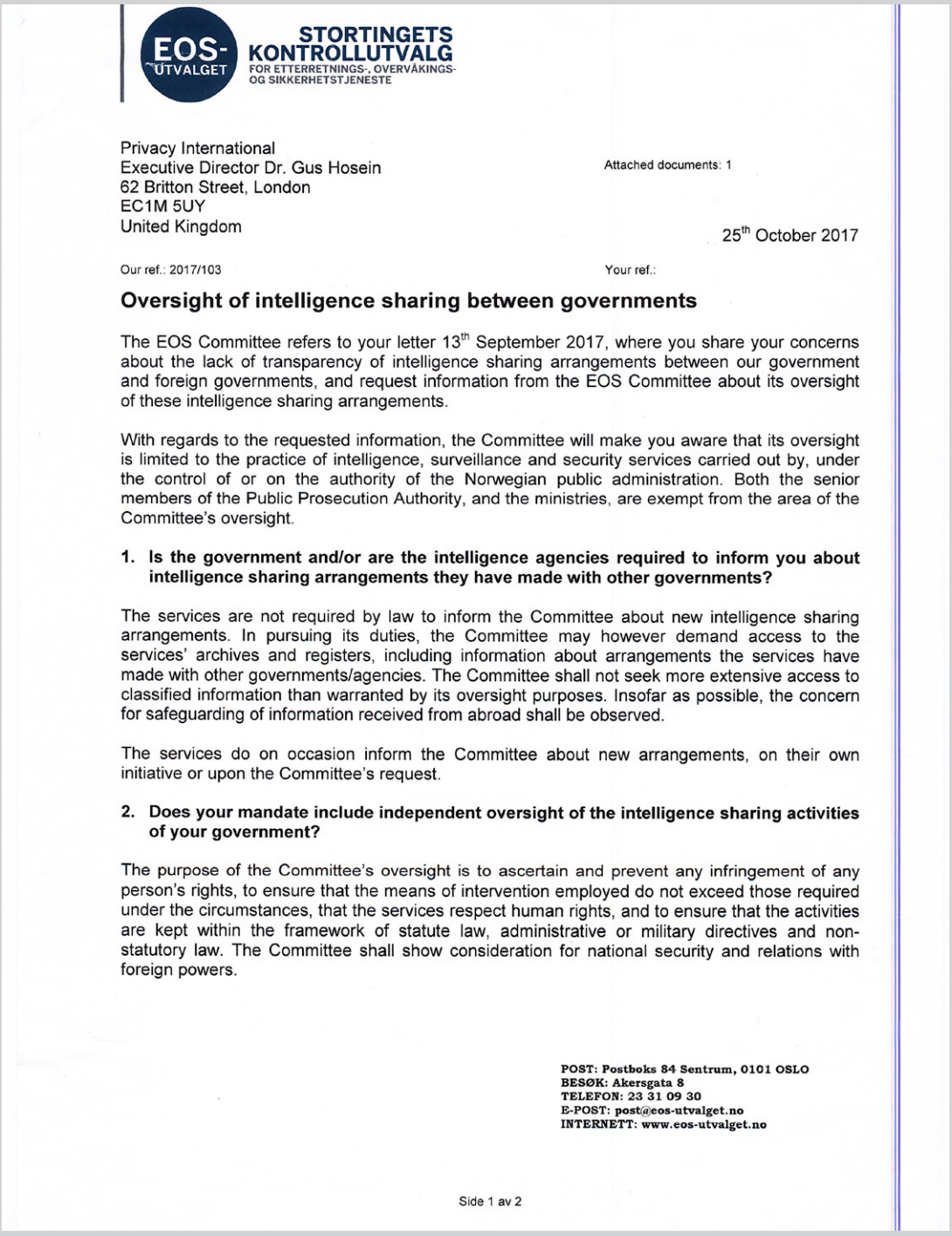
5. **Do you cooperate with any oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government?**

No, the ISC does not have this statutory function. The ISC's functions are set out above in response to your second question.

I trust this information is helpful.

Yours sincerely

Andrew Kibblewhite
Chief Executive
Department of the Prime Minister and Cabinet



EOS-UTVALGET
STORTINGETS KONTROLLUTVALG
FOR ETTERRETNINGS-, OVERVÅKINGS- OG SIKKERHETSTJENESTE

Privacy International
Executive Director Dr. Gus Hosein
62 Britton Street, London
EC1M 5UY
United Kingdom

Attached documents: 1

25th October 2017

Our ref.: 2017/103

Your ref.:

Oversight of intelligence sharing between governments

The EOS Committee refers to your letter 13th September 2017, where you share your concerns about the lack of transparency of intelligence sharing arrangements between our government and foreign governments, and request information from the EOS Committee about its oversight of these intelligence sharing arrangements.

With regards to the requested information, the Committee will make you aware that its oversight is limited to the practice of intelligence, surveillance and security services carried out by, under the control of or on the authority of the Norwegian public administration. Both the senior members of the Public Prosecution Authority, and the ministries, are exempt from the area of the Committee's oversight.

1. **Is the government and/or are the intelligence agencies required to inform you about intelligence sharing arrangements they have made with other governments?**

The services are not required by law to inform the Committee about new intelligence sharing arrangements. In pursuing its duties, the Committee may however demand access to the services' archives and registers, including information about arrangements the services have made with other governments/agencies. The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes. Insofar as possible, the concern for safeguarding of information received from abroad shall be observed.

The services do on occasion inform the Committee about new arrangements, on their own initiative or upon the Committee's request.

2. **Does your mandate include independent oversight of the intelligence sharing activities of your government?**

The purpose of the Committee's oversight is to ascertain and prevent any infringement of any person's rights, to ensure that the means of intervention employed do not exceed those required under the circumstances, that the services respect human rights, and to ensure that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law. The Committee shall show consideration for national security and relations with foreign powers.

POST: Postboks 84 Sentrum, 0101 OSLO
BESØK: Akersgata 8
TELEFON: 23 31 09 30
E-POST: post@eos-utvalget.no
INTERNETT: www.eos-utvalget.no

Within this framework, the Committee oversees the intelligence sharing activities of the services. This includes assessments of whether or not the services have complied with relevant regulations and policies when disclosing information to other services, domestic or foreign.

3. **Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?**

See question 1 above.

4. **Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government?**

The Committee is not authorized to order the services to take specific action on a matter, nor to make decisions to which the services are obligated to conform. The Committee may express its opinion on matters or situations it investigates as part of its oversight duties and make recommendations to the services, such as recommending that a practice or measure ought to be discontinued. The Committee will report its findings to the Parliament, which can then decide if changes in legislation or practices are necessary. The Committee shall, as a rule, conform to the principle of subsequent oversight. However, the Committee may demand access to, and comment on, current issues.

These procedures apply to the oversight of the services' intelligence sharing activities as well. In the Committee's annual report for 2016 to the Parliament, the Committee criticized the Police Security Service for matters concerning international sharing of intelligence information.[1]

5. **Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government?**

The Committee has found that having contact with similar oversight bodies in other countries has been fruitful in the sense of getting new ideas and methods for performing oversight.

In the Committee's view there should be considered whether (and if so, how) it is possible to have more systematic collaboration between oversight bodies, without infringing on the rules of secrecy that the oversight bodies are bound by.

***

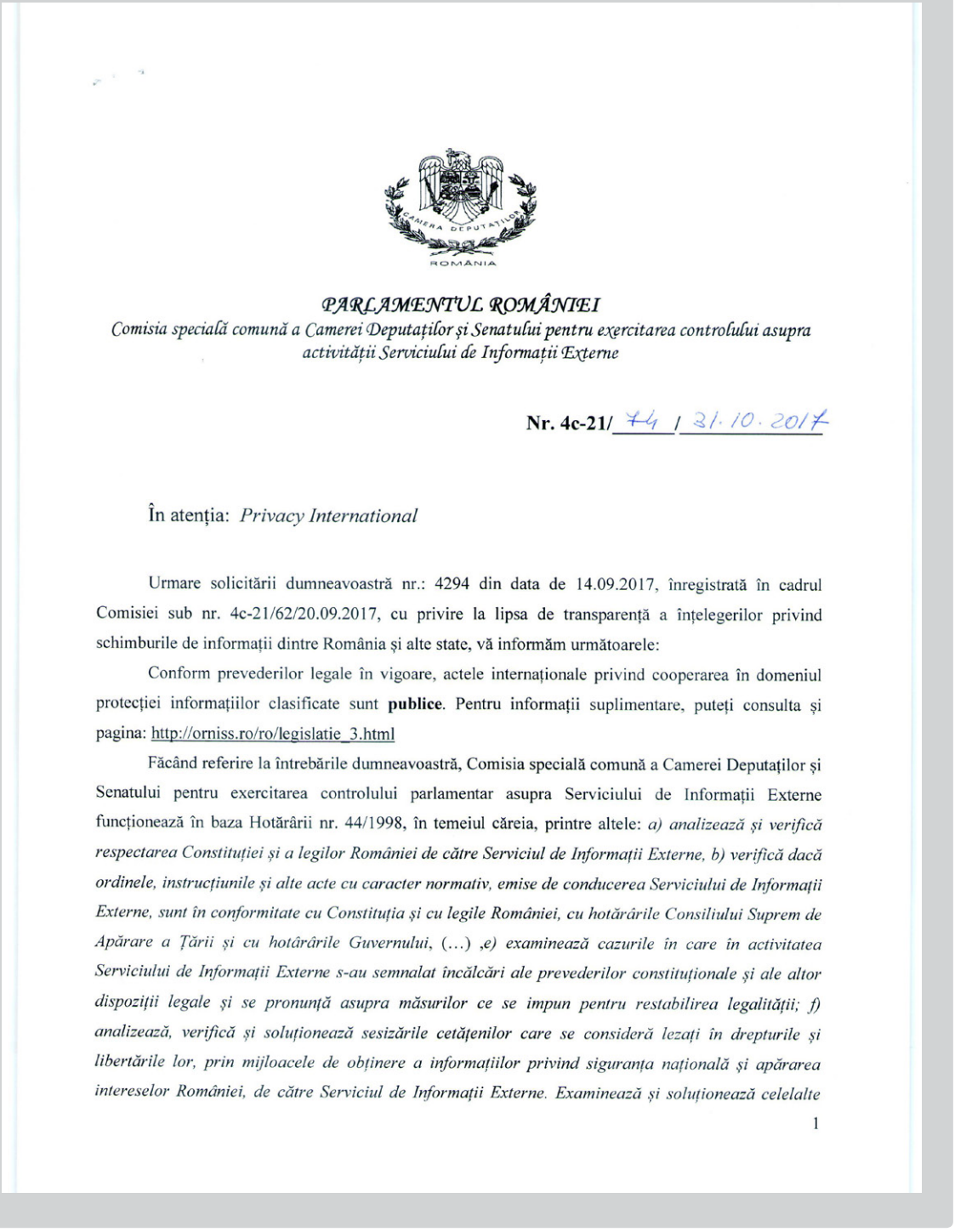
The Committee has contributed to the book "Making International Intelligence Cooperation Accountable", written by Hans Born, Ian Leigh and Aidan Wills, published in 2015. A copy of the book is enclosed. For more information on the EOS Committee's oversight of international intelligence cooperation, see especially chapter 7.

Yours sincerely,

Eldbjørg Løwer
Committee Chair

[1] See chapter 4.9 in the Committee's "Annual report 2016". The report can be downloaded from our website: eos-utvalget.no.

Side 2 av 2



PARLAMENTUL ROMÂNIEI

Comisia specială comună a Camerei Deputaților și Senatului pentru exercitarea controlului asupra activității Serviciului de Informații Externe

Nr. 4c-21/ 74 / 31.10.2017

În atenția: *Privacy International*

Urmare solicitării dumneavoastră nr.: 4294 din data de 14.09.2017, înregistrată în cadrul Comisiei sub nr. 4c-21/62/20.09.2017, cu privire la lipsa de transparență a înțelegerilor privind schimburile de informații dintre România și alte state, vă informăm următoarele:

Conform prevederilor legale în vigoare, actele internaționale privind cooperarea în domeniul protecției informațiilor clasificate sunt **publice**. Pentru informații suplimentare, puteți consulta și pagina: http://orniss.ro/ro/legislatie_3.html

Făcând referire la întrebările dumneavoastră, Comisia specială comună a Camerei Deputaților și Senatului pentru exercitarea controlului parlamentar asupra Serviciului de Informații Externe funcționează în baza Hotărârii nr. 44/1998, în temeiul căreia, printre altele: *a) analizează și verifică respectarea Constituției și a legilor României de către Serviciul de Informații Externe, b) verifică dacă ordinele, instrucțiunile și alte acte cu caracter normativ, emise de conducerea Serviciului de Informații Externe, sunt în conformitate cu Constituția și cu legile României, cu hotărârile Consiliului Suprem de Apărare a Țării și cu hotărârile Guvernului, (...) ,e) examinează cazurile în care în activitatea Serviciului de Informații Externe s-au semnalat încălcări ale prevederilor constituționale și ale altor dispoziții legale și se pronunță asupra măsurilor ce se impun pentru restabilirea legalității; f) analizează, verifică și soluționează sesizările cetățenilor care se consideră lezați în drepturile și libertățile lor, prin mijloacele de obținere a informațiilor privind siguranța națională și apărarea intereselor României, de către Serviciul de Informații Externe. Examinează și soluționează celelalte*

1

plângeri și sesizări care îi sunt adresate în legătură cu încălcarea legii de către Serviciul de Informații Externe; (...)

În exercitarea atribuțiilor de îi revin, Comisia este îndreptățită să solicite Serviciului de Informații Externe, prin intermediul directorului acestuia, documente, date și informații și poate audia orice persoană în legătură cu problemele analizate. În acest context, Serviciul de Informații Externe este obligat să răspundă în timp util solicitărilor Comisiei și să permită audierea persoanelor indicate de aceasta, cu acordul prealabil al directorului Serviciului de Informații Externe, ***exceptând*** documentele, datele și informațiile în legătură cu acțiunile informative privind siguranța națională, aflate în curs sau care urmează a fi executate, apreciate ca atare de către Comisie, la recomandarea Consiliului Suprem de Apărare a Țării, precum și informațiile care pot conduce la deconspirarea calității reale a cadrelor operative, la identificarea surselor de informare, a metodelor și mijloacelor de muncă concrete folosite în munca de informații, în măsura în care acestea nu contravin Constituției și legislației în vigore.

În plus, conform articolului 2 alin. (1) din Legea nr. 1/1998 privind organizarea și funcționarea Serviciului de Informații Externe, *"Serviciul de Informații Externe face parte din sistemul național de apărare. Activitatea sa este organizată și coordonată de Consiliul Suprem de Apărare a Țării"*. Conform articolului 4 alin. (2) din aceeași lege, *"Cu aprobarea Consiliului Suprem de Apărare a Țării Serviciul de Informații Externe poate stabili relații cu organisme similare din străinătate"*. Astfel, în ceea ce privește accesul membrilor Comisiei la informațiile relevante legate de schimburile de informații alte statului, în sfera atribuțiilor ce-i revin și prin prisma cazurilor concrete supuse atenției Comisiei, aceste informații pot fi obținute *la cerere și cu acordul părților implicate.*

Totodată, Comisia cooperează cu alte organisme de control, naționale și străine, în speță concrete supuse atenției acesteia.

Cu deosebită stimă,

PREȘEDINTE,

Deputat Mihai Weber

2

This document is an unofficial translation from Romanian by the Asociația pentru Tehnologie și Internet of the original text.

Concerning your request no. 4294 from 14.09.2017, registered at the committee under no. 4c-21/62/20.09/2017, regarding the lack of transparency of the intelligence sharing agreements between Romania and other countries, we inform you the following:

According to the current legislation, the international documents concerning cooperation in the field of classified information are **public**. For more information, you can go to the following web page: http://orniss.ro/ro/legislatie_3.html

Referring to your questions, the The Joint Standing Committee for the exercise of parliamentary control over the activity of the Foreign Intelligence Service does its work according to Decision no. 44/1998, based on which, among others, it:
a) analyzes and verifies the compliance with the Constitution and the laws of Romania by the Foreign Intelligence Service,
b) verifies that the orders, instructions and other regulatory documents (i.e. secondary legislation - translation note) put forward by the leadership of the Foreign Intelligence Service comply with the Constitution and the laws of Romania, the decisions of the Supreme Defense Council and the decisions of the Government, (…)
e) examines the cases where infringements on the provisions of the Constitution or on other legal provisions have been reported during the activity of the Foreign Intelligence Service and decides on the measures necessary to restore compliance with the law;
f) analyzes, verifies and solves the complaints of citizens who deem to have had their rights and freedoms infringed upon by way of the means of gathering intelligence regarding national security and the defense of Romania's interests by the Foreign Intelligence Service and solves any other complaints and notifications addressed to it regarding infringements of the law by the Foreign Intelligence Service; (…)

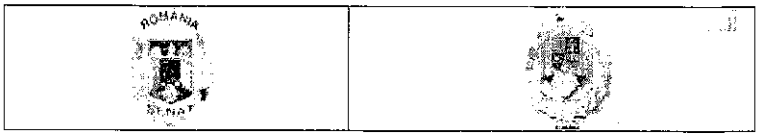
In exercising its duties, the Committee has the right to ask the Foreign Intelligence Service, through its director, for documents, data and information and it can organize hearings of any person related to the analyzed problems. Within this context, the Foreign Intelligence Service is obligated to answer in due time to the inquiries of the Committee and to permit the hearing of the persons indicated by it, with the previous agreement of the director of the Foreign Intelligence Service, **with the exception of** the documents, data and information related to currently ongoing or future national security intelligence activities, considered as such by the Committee at the recommendation of the Supreme Defense Council, as well as the information which could lead to breaking of the cover of operatives, to the identification of sources, of concrete methods and means of work used in intelligence gathering, to the extent that these do not infringe on the Constitution and standing legislation.

Moreover, according to article 2.(1) of Law no. 1/1998 concerning the organization and functioning of the Foreign Intelligence Service, “The Foreign Intelligence Service is part of the national defense system. Its activity is organized and coordinated by the Supreme Defense Council”. According to article 4.(2) of the same law, “With the approval of the Supreme Defense Council, the Foreign Intelligence Service can establish relationships with similar foreign organizations”. So, concerning the access of the Committee's members to relevant information regarding state intelligence sharing, given its purview and the concrete situations which came to the attention of the Committee, these informations can be obtained upon *request and with the accord of the involved parties*.

Furthermore, the Committee cooperates with other oversight bodies, both national and foreign, in cases brought to its attention.

Respectfully,

President,
Deputy Mihai Weber



Parlamentul României

Comisia comună permanentă a Camerei Deputaților și Senatului pentru exercitarea controlului parlamentar asupra activității Serviciului Român de Informații

Nr.4c-20/586/08.11.2017

Către: PRIVACY INTERNATIONAL

ApTI (Asociația pentru Tehnologie și Internet)

Urmare a adresei dvs. Nr. 4c-20/586/14.09.2017, Comisia comună permanentă a Camerei Deputaților și Senatului pentru exercitarea controlului parlamentar asupra activității Serviciului Român de Informații (Comisia) a analizat cu atenție petiția dvs. și a procedat la cercetarea aspectelor semnalate.

În ședința din data de 1 noiembrie 2017 membrii Comisiei au formulat următoarele răspunsuri:

1. **La întrebarea dvs. privind obligația Guvernului și/sau a serviciilor de informații de a informa Comisia în legătură cu înțelegerile privind schimbul de informații pe care le-au încheiat cu alte guverne/state, vă comunicăm următoarele:**

Atribuțiile Comisiei sunt exercitate doar în raport cu SRI și nu cu Guvernul sau cu alte servicii de informații. În conformitate cu Art. 1. alin. (3) din HP nr. 30/1993 privind organizarea și funcționarea Comisiei, Comisia are atribuții privind supravegherea îndeplinirii de către Serviciul Român de Informații (SRI) a misiunilor ce îi revin în conformitate cu prevederile legale în vigoare și efectuează un control concret și permanent asupra activităților SRI. Pe lângă alte atribuții, Comisia monitorizează modul de îndeplinire de către SRI a cerințelor legale în ceea ce privește măsurile care presupun restrângerea exercițiului drepturilor și libertăților cetățenești.

Conform Art. 4. lit. f) din HP nr. 30/1993, Comisia examinează rapoartele prezentate Parlamentului, potrivit legii, de către directorul SRI și întocmește un raport propriu asupra acestora, pe care îl înaintează birourilor permanente ale celor două Camere ale Parlamentului.

În cadrul controlului parlamentar, Comisia verifică dacă, în exercitarea atribuțiilor ce revin SRI sunt respectate prevederile Constituției și ale celorlalte acte normative, respectiv modul în care SRI asigură respectarea, în cadrul activității de informații, a drepturilor și libertăților persoanelor.

SRI este obligat – conform Art. 6 din HP nr. 30/1993 - să pună la dispoziția Comisiei în șapte zile rapoartele, informările, explicațiile, documentele, datele și informațiile solicitate și să permită audierea personalului militar și civil indicat de Comisie, dacă este cazul. Sunt exceptate documentele, datele și informațiile în legătură cu acțiunile informative privind securitatea națională, aflate în curs sau care urmează a fi executate, precum și informațiile care pot conduce la deconspirarea calității reale a cadrelor operative, la identificarea surselor de informare, a metodelor și mijloacelor de muncă concrete folosite în activitatea de informații. Nu fac obiectul excepției acele situații în care un organ judiciar a constatat încălcarea unor drepturi sau libertăți cetățenești.

Având în vedere cele de mai sus, vă informăm că nu există prevederi exprese prin care SRI să fie obligat să informeze Comisia în legătură cu înțelegerile privind schimbul de informații pe care SRI le-a încheiat cu alte guverne/state, dar, dacă există indicii rezonabile că prin respectivele înțelegeri au fost restrânse drepturile și libertățile cetățenești, Comisia are dreptul să efectueze verificări și să solicite SRI explicații și documente relevante, așa cum se menționează mai sus.

2. **La întrebarea dvs. în legătură cu existența unui mandat al Comisiei pentru efectuarea unui control independent al activităților de schimb de informații ale Guvernului/Statului, vă comunicăm următoarele:**

Reiterăm afirmația de mai sus și anume că atribuțiile Comisiei sunt exercitate doar în raport cu SRI și nu cu Guvernul/Statul. Pe cale de consecință, nu există un mandat general încredințat Comisiei pentru a efectua un control independent al activităților de schimb de informații ale Guvernului/Statului.

3. **La întrebarea dvs. în legătură cu abilitarea Comisiei de a avea acces la toate informațiile relevante legate de schimburile de informații ale Guvernului/Statului, vă comunicăm următoarele:**

Comisia poate solicita SRI rapoarte, informări, explicații, documente, date, informații, etc. iar SRI are obligația de a le pune la dispoziția Comisiei, cu excepția menționată mai sus, la răspunsul la întrebarea nr. 1.

4. **La întrebarea dvs. în legătură cu abilitarea Comisiei de a revizui deciziile privind schimbul de informații și/sau de a desfășura investigații independente în legătură cu activitățile de schimb de informații ale Guvernului/Statului, vă comunicăm următoarele:**

Schimbul de informații ale Guvernului/Statului cu alte state se realizează în baza unor acorduri bilaterale sau multilaterale.

În conformitate cu HP 30/1993, Art. 4 lit. c) Comisia examinează cazurile în care s-au semnalat încălcări ale prevederilor constituționale și ale altor dispoziții legale în activitatea Serviciului Român de Informații și se pronunță asupra măsurilor ce se impun pentru restabilirea legalității. Pe cale de consecință, dacă s-ar impune revizuirea deciziilor privind schimbul de informații, acest lucru se poate face prin modificarea acordurilor de către părțile semnatare din cadrul Guvernului/Statului.

5. **La întrebarea dvs. în legătură cu cooperarea Comisiei cu alte organisme de control naționale sau străine, pentru controlul activităților de schimb de informații ale Guvernului/Statului, vă comunicăm următoarele:**

În România, prin Legea nr. 64/2013 a fost ratificat acordul dintre statele membre ale Uniunii Europene, reunite în cadrul Consiliului, privind protecția informațiilor clasificate schimbate în interesul Uniunii, semnat la Bruxelles, la data de 25 mai 2011.

În general, prin ratificarea acordurilor încheiate între România și alte state, se creează cadrul normativ necesar asigurării protecției reciproce a informațiilor clasificate schimbate sau produse în procesul de cooperare între părți. De regulă, aceste acorduri creează un set de reguli aplicabil tuturor activităților de cooperare și contractelor viitoare care vor fi implementate între părți și care vor conține, sau vor implica informații clasificate. Acordurile reglementează:

a) scopul și domeniul de aplicare;
b) autoritățile competente de securitate[1];
c) echivalența gradelor de secretizare;
d) condițiile de acces la informațiile clasificate;

[1] *În România, autoritatea competentă este Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS), instituție publică având personalitate juridică, în subordinea Guvernului României și în coordonarea directă a Prim-ministrului, cu autoritate la nivel național în domeniul securității informațiilor clasificate. ORNISS asigură implementarea unitară, la nivel național, a măsurilor de securitate a informațiilor naționale clasificate, precum și a celor echivalente care fac obiectul tratatelor, înțelegerilor și acordurilor bilaterale sau multilaterale la care România este parte. ORNISS este organismul național de legătură pentru informațiile clasificate cu Oficiul de Securitate al NATO (NOS), cu structurile de securitate similare din statele membre și partenere ale NATO, ale UE și ale altor organizații internaționale precum și cu cele ale statelor cu care România a încheiat tratate, înțelegeri sau acorduri care prevăd protecția informațiilor clasificate.*

e) măsurile de protecție a informațiilor clasificate;
f) încheierea și derularea contractelor clasificate de către o parte sau o persoană juridică dintr-un stat pe teritoriul celeilalte părți;
g) cercetarea și soluționarea incidentelor de securitate.

Potrivit art. 25 alin. 5 din Legea nr. 182/2002 privind protecția informațiilor clasificate, protecția informațiilor nedestinate publicității transmise României de alte state sau organizații internaționale, respectiv accesul la aceste informații, se realizează în condițiile statuate prin tratatele internaționale sau prin acordurile la care țara noastră este parte.

Astfel, schimbul de informații între SRI și servicii de informații partenere din alte state se realizează conform regulilor instituite prin protocoalele de cooperare încheiate de către SRI cu organisme similare din străinătate, cu respectarea normelor în vigoare. Acordurile încheiate de țara noastră, respectiv protocoalele la care SRI este parte, statuează expres obligația respectării regulii "terței părți" potrivit căreia, în orice activitate care presupune cooperare/schimb de informații, transmiterea unei informații clasificate către o terță entitate se realizează exclusiv cu acordul părții emitente.

Vă mulțumim pentru încrederea acordată, asigurându-vă de întreaga noastră disponibilitate pentru examinarea și clarificarea oricăror cazuri în care sunt semnalate încălcări ale prevederilor constituționale și/sau ale altor dispoziții legale în activitatea Serviciului Român de Informații.

Cu stimă,

Senator Iulian-Claudiu MANDA

PREȘEDINTE

This document is an unofficial translation from Romanian by the Asociația pentru Tehnologie și Internet of the original text.

Concerning your request no. 4c-20/586/14.09/2017, the The Joint Standing Committee of the Chamber of Deputies and of the Senate for the exercise of parliamentary control over the activity of the Romanian Intelligence Service (the Committee) carefully analyzed your petition and proceeded to investigate the mentioned issues.

In the meeting from 1 November 2017, the Committee's members formulated the following answers:

1. To your question regarding the obligation of the Government and/or of the intelligence agencies being required to inform the Committee about intelligence sharing arrangements made with other governments/states, our answer is the following:

The Committee's competences are exercised only in relation to the SRI[1], not in relation with the Government or any other intelligence services. According to article 1.(3) of Parliament Decision no. 30/1993 regarding the organization and functioning of the Committee, the Committee has competences overseeing that the Romanian Intelligence Service (SRI) fulfils its duties according to the current legal provisions and performs a concrete and permanent control of SRI's activities. Among others, the Committee monitors the way SRI comply with the legal requirements regarding measures which involve the limitations of the exercise of citizens' rights and freedoms.

According to article 4.f) of Parliament Decision no. 30/1993, the Committee examines reports presented to the Parliament, according to the law, by the SRI director and drafts its own report regarding them, which it then forwards to the Standing Bureaus of both chambers of the Parliament.

As part of parliamentary oversight, the Committee checks if, during the course of the work SRI does, the provisions of the Constitution and of the rest of the legislation are followed, as well as the way SRI upholds the rights and freedoms of the individuals during its intelligence activities.

SRI is obligated – according to article 6 of Parliament Decision no. 30/1993 – to provide the Committee within 7 days the requested reports, briefings, explanations, documents, data and information and to permit the hearing of military and civilian personnel indicated by the Committee, if that is the case. The documents, data and information related to currently ongoing or future national security intelligence activities, considered as such by the Committee at the recommendation of the Supreme Defense Council, as well as the information which could lead to breaking of the cover of operatives, to the identification of sources, of concrete methods and means of work used in intelligence gathering. The situations when a court of law decides that there have been infringements upon civil rights or freedoms taking place are not covered by the previously described exception.

Taking all of the above into consideration, we inform you that there are no explicit provisions mandating that the SRI needs to inform the Committee about intelligence sharing agreements it has established with other governments/states, but, if there are reasonable indications that

through these agreements civil rights and freedoms have been infringed upon, the Committee has the right to check and to ask SRI for explanations and relevant documents, like described earlier.

2. To your question about the existence of a mandate of the Committee for performing independent oversight of the intelligence sharing activities of the government/state, our answer is the following:

We reiterate the statement from above, namely that the Committee's competences are exercised only in relation to the SRI, not in relation with the Government/State. As a consequence, there is no general mandate given to the Committee to perform an independent control of the intelligence sharing activities of the Government/State.

3. To your question about the ability of the Committee to access in full all relevant information about the intelligence sharing activities of the Government/State, our answer is the following:

The Committee can ask SRI for reports, briefings, explanations, documents, data, information etc. and the SRI has the obligation to provide them to the Committee, with the exception mentioned earlier, in the answer to question no. 1.

4. To your question about the ability of the Committee to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of the Government/State, our answer is the following:

The information sharing of the Government/State with other states is done based on bilateral and multilateral accords.

According to Parliament Decision 30/1993, article 4.c) the Committee examines the cases where infringements of the constitutional or legal provisions have been reported during the activity of the Romanian Intelligence Service and decides on the measures necessary to restore observance of the law. As a consequence, if an update of the intelligence sharing framework would be needed, this can be done by modifying the agreements by the signatory organisations of the Government/State.

5. To your question about the Committee's cooperation with other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of the Government/State, our answer is the following:

In Romania, Law no. 64/2013 ratified the agreement between the European Union's Member States, gathered at the Council of the European Union, regarding the protection of classified information shared in the interest of the Union, signed at Brussels on 25 May 2011.

In general, through the ratification of agreements between Romania and other states, a legal framework necessary for providing reciprocal protection of classified information shared or created during the cooperation process amongst partners is created. Usually, these agreeements establish a set of rules applicable to all cooperation activities and to all future contacts which will take place between partners and which will contain, or involve classified information. The accords regulate:
a) the purpose and scope of the accords;
b) the competent security authorities[2];
c) the equivalence of classification levels;
d) the access conditions to classified information;
e) the protection measures for classified information;
f) the establishment and execution of classified contracts by a party or legal person from a state on the territory of the other party;
g) the research and solving of security incidents.

According to article 25.(5) of Law no. 182/2002 regarding the protection of classified information, the protection of non-public information transmitted to Romania by other states or international organizations, and the access to this information, is done according to rules established by international treaties or agreements to which our country is party.

Thus, intelligence sharing between SRI and partner intelligence services from other countries are done according to the rules established through cooperation protocols between SRI and similar foreign organizations, while respecting established norms. The agreements established by our country, including the protocols SRI is a party of, explicitly state the obligation to respect the "third party" rule which says that, in any activity involving cooperation/intelligence sharing, the communication of a piece of classified information to a third party is done exclusively with the agreement of the sending party.

Thank you for your trust. We assure you of our availability for examining and clarifying any cases involving reports of infringements upon constitutional and/or legal provision during the activity of the Romanian Intelligence Service.

Respectfully,

Senator Iulian-Claudiu MANDA
PRESIDENT

[1] SRI – Serviciul Român de Informaţii – Romanian Intelligence Service

[2] In Romania, the competent authority is the Office of the National Registry of State Secret Information – Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS), a public institution having legal personality, subordinated to the Romanian Government and under the direct coordination of the Prime-minister, with national authority on matters related to classified information. ORNISS provides an unitary implementation, at the national level, for the security measures of national classified information, as well as equivalent one which fall under the purview of bilateral or multilateral treaties, agreements and accords to which Romania is a party. ORNISS is the national liaison organization to the NATO Security Office – Oficilul de Securitate al NATO (NOS) on classified information issues., to similar security structures in NATO member states and partners, in EU Member States and other international organizations, as well as states with which Romania has treaties, agreements an accords involving the protection of classified information.

REPUBLIC OF SLOVENIA
INFORMATION COMMISSIONER
Zaloška 59, 1000 Ljubljana, Slovenia
T: (+386) 1 230 9730
F: (+386) 1 230 9778
gp.ip@ip-rs.si
www.ip-rs.si

Number: 542-1/2017/160
Date: 4.10.2017

Digitalno podpisal Informacijski pooblaščenec
DN: c=si, o=state-institutions, ou=web-certificates, ou=Government, serialNumber=1237034018018, cn=Informacijski pooblaščenec
Datum: 2017.10.04 14:15:26 +02'00'

Privacy International
Scarlet Kim
scarlet@privacyinternational.org

Državljan D
Domen Savič
[redacted]

Subject: Oversight of intelligence sharing between Slovene government and foreign governments - Slovenia

Dear Dr. Hosein and Mr. Savič,

the Information Commissioner (IC) has received your Briefing to National Intelligence Oversight Bodies and related questions with request for non-confidential work products of the Information Commissioner reflecting the answers on the supervision of the intelligence agencies in the Republic of Slovenia. Please find the answers of the Information Commissioner below.

1. *Is the government and/or are the intelligence agencies required to inform you about intelligence sharing arrangements they have made with other governments?*

No.

2. *Does your mandate include independent oversight of the intelligence sharing activities of your government?*

In a very limited scope but in no way fully. The competences of the IC are strictly limited to the supervision of the processing of personal data as defined by the Personal data protection act (PDPA)[1]. The competences of the IC are defined by the Information Commissioner Act[2]. In that context all the data controllers are covered in this supervision since the PDPA does not discriminate between different controllers or exclude any of them. The Constitutional court of the Republic of Slovenia has however strictly defined the limit of these inspection supervisory activities and instructed the IC not to interfere with any official procedures in the context of this supervision (Decision of the Constitutional Court of the Republic of Slovenia N. U-I-92/12-13, 10. 10. 2013[3]). In that context please see the request to initiate the procedure for the review of the constitutionality and legality of regulations or general acts, which the IC has submitted to the Constitutional Court of RS with relation to the constitutionality of the Slovene Intelligence and Security Agency Act (ZSOVA[4]).

Since by nature of such activities the main scope of the activities of the Slovene Intelligence and Security Agency (SOVA)[5] as well as any other activities of the Slovene government related to intelligence sharing is mostly related to the constitutionally guaranteed right to the Protection of the Privacy of Correspondence and Other Means of Communication (Article 37 of the Constitution of the Republic of Slovenia[6]) and in a very limited scope to the constitutionally guaranteed right to the Protection of personal data (Article 38 of the Constitution of the Republic of Slovenia) the mandate of

[1] https://www.ip-rs.si/en/legislation/personal-data-protection-act/
[2] https://www.ip-rs.si/en/legislation/information-commissioner-act/
[3] http://odlocitve.us-rs.si/sl/odlocitev/US30234?q=U-I-92%2F12-13
[4] https://www.ip-rs.si/fileadmin/user_upload/Pdf/mnenja/Zahteva_za_oceno_ustavnosti.pdf
[5] http://www.sova.gov.si/en/
[6] http://www.us-rs.si/en/about-the-court/legal-basis/

1

the IC in relation to the independent oversight of the intelligence sharing activities of Slovene government is rather limited. This is further enhanced by the fact that the main supervisory body legally entrusted with the supervision of the whole work of the main body entrusted by law with such activities, namely Slovene Intelligence and Security Agency (SOVA)[7], is the Commission for the Supervision of Intelligence and Security Services (KNOVS[8]) as defined and regulated by the Parliamentary Supervision of the Intelligence and Security Services Act[9].

3. *Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?*

No. IC has only limited access in relation to the IC's competences which is independent supervision of the processing of personal data as defined by the Personal data protection act[10]. This does not (as already mentioned) include the overall supervision of the intelligence sharing activities of the Slovene government.

4. *Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government?*

The Slovene government is by law not required to consult us on the decisions to share intelligence. The IC is by law not authorised to review these decisions in full or to abolish them. The IC could review such decisions only if it became aware of such decisions either as mentioned in the context of its competences (which is independent supervision of the processing of personal data as defined by the Personal data protection act) or otherwise give opinion as defined by the Article 48 of the PDPA on the aspect of the processing of personal data. But the IC could not review such decisions with any legal implications.

5. *Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government?*

We do not have the competences to officially cooperate in this context, but we do cooperate fully as independent supervisory body for personal data protection in the Working party 29 and all EU established supervisory bodies (such as supervision of Schengen - SIS II Supervision Coordination Group, Europol cooperation board, Eurodac Supervision Coordination Group and VIS Supervision Coordination Group). Our efforts to co-operate with domestic oversight bodies, namely with the above-mentioned Commission for the Supervision of Intelligence and Security Services (KNOVS) were not met with appreciation. IC tried to share our findings of the SOVA investigation with KNOW, which however rejected to become aware of the findings. Given that this path was not successful and that the government did not fulfil its promise to amend the act on SOVA, the IC lodged the request with the Constitutional court to review the constitutionally of the Slovene Intelligence and Security Agency Act (ZSOVA).

Kind regards,

Mojca Prelesnik,
Information Commissioner

[7] http://www.sova.gov.si/en/
[8] https://www.dz-rs.si/wps/portal/en/Home/ODrzavnemZboru/KdoJeKdo/DelovnoTelo?idDT=DT009
[9] http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455
[10] https://www.ip-rs.si/en/legislation/personal-data-protection-act/

DEFENSOR DEL PUEBLO
EL SECRETARIO GENERAL

Defensor del Pueblo
REGISTRO
Fecha: 24 Octubre 2017
Salida: 17104657

Sra. D.ª SCARLET KIM
Asesora Jurídica de **Privacy International**
scarlet@privacyinternational.org

17057344

Estimada señora:

Se ha recibido su escrito, en el que plantea la falta de transparencia de los acuerdos de intercambio de inteligencia entre gobiernos y solicita información sobre la supervisión de dichos acuerdos.

El Defensor del Pueblo tiene encomendada por el artículo 54 de la Constitución y por la Ley Orgánica 3/1981, de 6 de abril, del Defensor del Pueblo, la defensa de los derechos comprendidos en el Título I de la Constitución y, a tal efecto, supervisa la actuación de las Administraciones públicas y el esclarecimiento de sus actos y resoluciones, así como de sus agentes, a la luz de lo dispuesto en el artículo 103.1 de la Constitución.

Para que el Defensor del Pueblo realizase la supervisión planteada en su escrito tendría que darse la circunstancia de alguna irregularidad administrativa concreta, ya que de forma genérica no podemos presumir que se hayan vulnerado los derechos y libertades fundamentales.

Si ustedes consideran que existen situaciones específicas que legitimen la intervención de esta institución pueden ponerlo en nuestro conocimiento para su valoración y, en su caso, posterior tramitación.

Le saluda atentamente,

José Manuel Sánchez Saudinós

Paseo de Eduardo Dato, 31 - 28010 Madrid (España)
Tel.:(+34) - 91 432 79 00 Fax: (+34) - 91 308 11 58
www.defensordelpueblo.es
registro@defensordelpueblo.es



Begin forwarded message:

From: [redacted]
Subject: **Regarding questions on intelligence oversight**
Date: 13 September 2017 at 15:31:44 BST
To: "tomasof@privacyinternational.org" <tomasof@privacyinternational.org>

Dear Mr. Falchetta,

We have received a letter from you regarding oversight of certain intelligence sharing arrangements.

The task for the Foreign Intelligence Court is to decide if collection of signals intelligence over airways and by cable for a specific task should be permitted or not. Hence the Court does not have any mandate to oversee intelligence sharing arrangements.

Since the Swedish Foreign Intelligence Inspectorate and the Swedish Commission on Security and Integrity Protection have certain supervisory tasks, they might be better suited to respond to your questions.

Yours sincerely,

[redacted]

SIUN
STATENS INSPEKTION FÖR FÖRSVARSUNDERRÄTTELSE-VERKSAMHETEN

2017-11-13

Diarienummer
71-2017Ö:3

Dr Gus Hosein, Privacy International
John Stauffer, Civil Rights Defenders

Angående tillsyn av svenskt samarbete med andra länder i underrättelsefrågor

Vi har mottagit ert brev av den 13 september 2017 avseende tillsyn av svenska försvarsmyndigheters samarbete med andra länder i underrättelsefrågor.

Statens inspektion för försvarsunderrättelseverksamheten (Siun) är den myndighet som har till uppgift att kontrollera att den försvarsunderrättelseverksamhet som bedrivs av Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut sker i enlighet med det av riksdagen och regeringen fastställda regelverket. Siuns granskning omfattar behandling av uppgifter som behandlas enligt lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (PUL UNDSÄK), samt enligt lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA PUL). Siun är även kontrollmyndighet enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen).

Siuns arbetsuppgifter och mandat regleras huvudsakligen i förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten (Siuns instruktion) samt i signalspaningslagen. Svaren nedan utgår därför från den konstitutionella situation som råder i Sverige.

Box 1140
164 22 Kista

Besöksadress:
Gullfossgatan 6

Telefon:
08-555 045 50

Fax:
08-555 045 60

E-post: registrator@siun.se
Webbplats: www.siun.se

Org. nr: 202100-6214

- I 3 § lagen (2000:130) om försvarsunderrättelseverksamhet anges att försvarsunderrättelsemyndigheterna, enligt regeringens närmare bestämmande, får etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer. I 3 § förordningen (2000:131) om försvarsunderrättelseverksamhet anges att samarbetet endast får ske under förutsättning att syftet med samarbetet är att tjäna den svenska statsledningen och det svenska totalförsvaret. De uppgifter som myndigheterna lämnar till andra länder och internationella organisationer får inte vara till skada för svenska intressen. I 6 § samma förordning anges att försvarsunderrättelsemyndigheterna ska informera Siun om de principer som tillämpas för samarbete i underrättelsefrågor med andra länder och internationella organisationer samt lämna uppgift om med vilka länder och organisationer sådant samarbete sker. Myndigheterna ska sedan samarbetet etablerats informera Siun om omfattningen av samarbetet och, när det bedöms vara motiverat, om resultatet, erfarenheterna och den fortsatta inriktningen av samarbetet. Utöver detta anges i 9 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet att signalspaningsmyndigheten även får, enligt regeringens närmare bestämmande, etablera och upprätthålla sådant internationellt samarbete på försvarsunderrättelseområdet - som avses i 3 § lagen om försvarsunderrättelseverksamhet (se ovan) - i sin utvecklingsverksamhet.

  Vidare finns regler i såväl PUL UNDSÄK som i FRA PUL som anger att personuppgifter som behandlas med stöd av lagarna får föras över till andra länder eller mellanfolkliga organisationer endast om sekretess inte hindrar det och det är nödvändigt för att Försvarsmakten respektive Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet, om inte regeringen meddelat föreskrifter eller i ett enskilt fall beslutat om att överföring får ske även i andra fall då det är nödvändigt för verksamheten vid respektive myndighet (1 kap. 17 § i båda lagarna). I förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, respektive förordningen (förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklings-

verksamhet anges att uppgifter får lämnas ut till en utländsk myndighet eller en internationell organisation, om utlämnandet tjänar den svenska statsledningen eller det svenska totalförsvaret. De uppgifter som Försvarsmakten respektive Försvarets radioanstalt lämnar till andra länder och internationella organisationer får inte vara till skada för svenska intressen (6 § respektive 7 § i förordningarna).

- Siuns mandat omfattar rätten att granska försvarsunderrättelsemyndigheternas samarbete i underrättelsefrågor.

- I 6 § Siuns instruktion anges att Siun har rätt att av myndigheter få de upplysningar och det biträde som behövs för dess verksamhet.

- Se ovan.

- Siun kan inom ramen för sin personuppgiftsgranskning anmäla ärenden till Datainspektion om det finns omständigheter som Datainspektion bör uppmärksammas på. Om Siun uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller juridisk person, ska Siun anmäla det till Justitiekanslern. Om Siun i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, ska Siun anmäla det till Åklagarmyndigheten (15 § Siuns instruktion).



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner FDPIC
The Deputy Commissioner

CH-3003 Berne, FDPIC, GL

Privacy International
Dr. Gus Hosein
Executive Director
62 Britton Street
GB - London, EC1M 5UY

E-mail: tomasof@privacyinternational.org
E-mail cc: scarlet@privacyinternational.org

Your references:
Our references: A2017.10.18-0007 / GL
Responsible: Caroline Gloor Scheidegger
Berne, 31.10.2017

Privacy International's letter and briefing on intelligence oversight

Dear Dr Hosein,

Thank you for your letter of 13 September 2017. We can answer your questions as follows:

Preliminary remarks:
On 1 September 2017, the new Intelligence Service Act (ISA) entered into force. Our authority was also consulted about the drafts and gave its opinion. You will find the Act ISA as well as its executing Ordinance on the internet in German, French and Italian.
In addition to the data protection supervision of our authority, the Federal Intelligence Service (FIS) is supervised by parliament, Federal Council, federal administration and the Federal Department of Defense Civil Protection and Sport (DDPS). The art. 76 – 78 ISA list in detail all competences of the independent supervision authority specially created to supervise the FIS. You will also find information in English concerning the Parliamentary Control Delegation in the internet, including a PDF concerning the Intelligence Oversight in Switzerland. In addition, the FIS has to guarantee a self-monitoring (art. 75 ISA). The FIS also has its own Data protection officer (DPO).

- **Is the government and/or are the intelligence agencies required to inform you about intelligence sharing arrangements they have made with other governments?**
  No. Art. 12 ISA regulates the cooperation with foreign governments/authorities. The federal Council can independently conclude international treaties about the international cooperation of the FIS concerning protection of information or the participation in international automated information systems (cf. art. 70 III ISA). Long-term intergovernmental administrative agreements concluded by the FIS with substantial financial consequences or due to legal or political reasons need an authorization by the Federal Council (cf. art. 80 III ISA). The FIS may conclude independently international agreements concerning minor technical issues (cf. art. 10 before mentioned Ordinance).

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

On the other hand, we have the opportunity to make a written statement during the office consulting procedure concerning the draft agreement.
We would also like to point out art. 61 ISA (communication of personal data to foreign authorities). The FIS has to take special guaranties before communicating personal data where the foreign legislation does not guaranty an adequate data protection level. Our authority has to be informed about such guaranties (cf. art. 6 III Federal Act on Data Protection FADP)
Finally, the above-mentioned Parliamentary Control Delegation has access to all documents concerning the FIS without restrictions, including intelligence sharing arrangements.

- **Does your mandate include independent oversight of the intelligence sharing activities of your government?**
  Our supervision competencies include the FIS. Only the Federal Council itself is excluded from our supervision (cf. art. 27 I FADP; concerning our independency, cf. art. 26 FADP; cf. also our preliminary remarks as well as our remarks to your first question).

- **Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?**
  Not directly, but within our legal scope (i.e. in relation with data protection resp. with the processing of personal data), we have the power to access all the information we need (cf. art. 27 FADP). As mentioned before, the Parliamentary Control Delegation has full access.

- **Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government?**
  Within our legal scope, we may recommend to end or modify the processing of personal data or to delete personal data. If a recommendation is not complied with or is rejected we may refer the matter to the department for a decision and finally we may appeal against this decision (cf. art. 27 V + VI FADP). Our Federal Data Protection law is currently being revised and the government bill foresees to give to our authority in general more power (among others that our authority will have the right to directly make decisions instead of recommendations).

- **Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government?**
  Up to now, no. However, we are in regular contact with the Parliamentary Control Delegation, the cantonal data protection authorities and the DPO of the FIS. We also know the other (foreign) data protection authorities and would cooperate, if needed.

We hope, having assisted you with this information. If you have any question, please do not hesitate to contact Ms Caroline Gloor Scheidegger (Caroline.gloorscheidegger@edoeb.admin.ch), legal advisor and head of the team 2 data protection.

Yours sincerely.

Jean-Philippe Walter

CC: Data protection officer (DPO) of the FIS

2/2

IPCO
Investigatory Powers Commissioner's Office

PO Box 29105, London
SW1V 1ZU

13 October 2017

FAO: Dr Gus Hosein, Renate Samson, Martha Spurrier & Jim Killock

By email to: scarlet@privacyinternational.org

Dear Sirs, Madams

Re: Oversight of intelligence sharing between Her Majesty's Government and foreign governments

I write in response to your letter of 13 September 2017 in which you collectively highlighted your concerns about the transparency of intelligence sharing arrangements between the UK and overseas governments. You also requested information about my oversight of these intelligence sharing arrangements.

Thank you for raising these important issues and also for your very useful briefing document on the issue of intelligence sharing. Your letter raises a number of very significant issues that I would like to address directly.

As you are aware, I am responsible for overseeing the use of investigatory powers by public authorities in the UK which include law enforcement, the intelligence agencies, prisons, local authorities and other government agencies. I am supported by 15 judicial commissioners as well as a broad range of support staff, including experienced inspectors and technical experts. On current plans, the total staff of the Investigatory Powers Commissioner's Office (IPCO) will be around 70 – twice the size of the three predecessor organisations. In addition to specific technical, legal and operational expertise, I am also recruiting an engagement team, with a view to improving transparency and maintaining a close working relationship with civil society and academia.

Having the powers set out in the answers below is not the same as using them, but there are two important ways that IPCO is different from previous organisations. I hope these will give you reassurance that we will be providing fully robust oversight. First, we will be larger and with greater expertise on technical and intelligence matters. Second, my powers of review – the 'double lock' – place a far greater onus, indeed a duty, on the intelligence agencies proactively to inform me of any relevant considerations when we conduct our review of a Secretary of State's decision to approve a warrant. Any planned or permitted disclosure is clearly a relevant consideration and I would expect it to be included in any application and will monitor that that occurs through our oversight powers.

Turning to your specific questions I will answer each in turn.

1. **Is the government and/or the intelligence agencies required to inform you about intelligence sharing arrangements they have made with other governments?**

   - Yes. You are aware that under the IPA 2016 All relevant persons have a statutory duty under s235 (ss (2), (3) & (4)) to provide my office with all information necessary to enable us to conduct our oversight function.

   - s208 IPA 2016 contains the relevant provisions for Judicial Commissioners to review and approve warrants for a number of powers. Any sharing of this intelligence would, we believe, be material to the proportionality case and so it is anticipated would form part of the warrant application reviewed by a Judicial Commissioner following approval by a Secretary of State.

   - We are also considering how any potential duty of candour upon the applicant will facilitate our oversight in this area. This is a matter we are currently working on.

2. **Does your mandate include independent oversight of the intelligence sharing activities of your government?**

   - Independence is at the heart of the new organisation; IPCO is an Arms Length Body of the Home Office but retains the authority to perform its statutory duties. My powers of oversight are derived from s229 of the IPA 2016 and, noting what I have said above, are I believe sufficient to oversee intelligence sharing. Should my view on this issue change, I will not be slow in identifying any perceived deficiencies.

3. **Do you have the power to access in full all relevant information about the intelligence sharing activities of your government?**

   - Yes. I have the power under s235 (2), (3) & (4) of the IPA to access any information relevant to my oversight. While my understanding is that the predecessor organisations have never been refused access to documentation that has been requested in respect of intelligence sharing, I intend to use these powers actively to ensure effective oversight.

   - The Act provides me with broad-ranging powers to request all the information I require to enable me to fulfil my functions effectively as Investigatory Powers Commissioner. I am exploring with those bodies I oversee how best to ensure a full understanding of their complete intelligence sharing activities. There are a number of possible approaches that could be taken to provide adequate oversight of sharing, including (but not limited to) - detailed analysis of sharing policies and any relevant undertakings set out contractually or in other agreements to assess whether these are adequate to protect individual rights; direct inspection of organisations not apparently covered by the IPA, but who are in receipt of material collected under IPA authorisation; agreements with partner oversight bodies that would shadow any sharing agreements, and, enable oversight to be carried out by partners on our behalf.

     Our initial view is that each of these approaches, and probably others not listed here, may be appropriate on a case by case basis depending on my assessment of the risk to individual rights in each situation.

4. **Do you have the power to review decisions to share intelligence and/or undertake independent investigations concerning the intelligence sharing activities of your government?**

- Yes. As part of my power of inspection under s229 (2) & (3a) of the IPA, I can review and undertake independent investigations of any sharing of intelligence. As set out above, the Act provides broad-ranging powers to undertake independent investigations and review decisions relating to intelligence-sharing arrangements.

5. Do you cooperate with any other oversight bodies, domestic or foreign, to oversee the intelligence sharing activities of your government?

- Cooperation between oversight bodies is something that I am committed to developing, however, it must be recognised that there are challenges due to the differing legislative regimes and issues around privacy and data sharing that will need to be explored. You will note that the Act specifically restricts me from doing anything that would undermine national security and, consequently, I am pursuing this work with care.

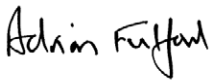
- I have held extremely positive discussions with oversight bodies from the 'Five Eyes' countries, including on the oversight of intelligence sharing. Preliminary discussions have led to a proposal to form a review body whose objectives include exchange of views on subjects of mutual interest and concern, the sharing of best practice in oversight methodology, and exploring areas where cooperation on reviews and the sharing of results is appropriate.

Finally, it is worth being aware of the Consolidated Guidance, which is designed to ensure that sharing of intelligence does not put someone in the position of their Article 3 rights being breached. This is something that I will continue to have oversight of, taking over from the Intelligence Services Commissioner's role in this regard.

IPCO has only existed since 1 September 2017 so I am regrettably unable at this stage to share 'non-confidential work products' which reflect my answers to the above questions. I intend, however, to cover the issue of intelligence sharing oversight in our first annual report. I am committed to transparency, wherever that is sensible and possible.

I trust my response answers the specific questions you have asked. Please do not hesitate to let me know if you have any further questions.

Yours



Rt Hon. Lord Justice Fulford
The Investigatory Powers Commissioner

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
WASHINGTON, D.C. 20427

December 22, 2017

Ms. Scarlet Kim
Legal Officer
Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

Dear Ms. Kim:

Thank you for your recent letter to the Privacy and Civil Liberties Oversight Board (PCLOB), which was sent on behalf of Privacy International, the Electronic Privacy Information Center (EPIC), the Center for Democracy & Technology (CDT), the Electronic Frontier Foundation (EFF), and the New America's Open Technology Institute (OTI). I also appreciate your sending a copy of the Briefing to National Intelligence Oversight Bodies titled, *"Human Rights Implications of Intelligence Sharing."*

Input from the privacy advocacy community has been crucial to the PCLOB's important work. Historically, the Board and individual Board Members have had numerous meetings with representatives of the advocacy community, which has provided valuable perspective on the PCLOB's work and projects that the Board undertakes.

As to your specific questions, PCLOB's authorizing statute vests the agency with robust authorities related to oversight of counterterrorism programs. The agency's authorities also include an advice function, whereby executive branch agencies are encouraged to consult with the PCLOB at an early stage of the development of a new policy, rule, or regulation. More information about the PCLOB's statutory authorities can be found on the agency's website: www.pclob.gov.

In performing its oversight and advice functions, the PCLOB has access to executive branch information within its mandate to review executive branch actions related to terrorism. We are committed to getting all the information we need to exercise our oversight and advice functions, and routinely work with other executive agencies to do so.

As an individual Board Member, I am committed to the critical mission of this agency: to ensure that the efforts by the Executive Branch to protect the nation from terrorism are balanced with the need to protect privacy and civil liberties. At the same time, I am committed to transparency in our work, consistent with the protection of our national security.

Ms. Scarlet Kim
Privacy International
Page 2

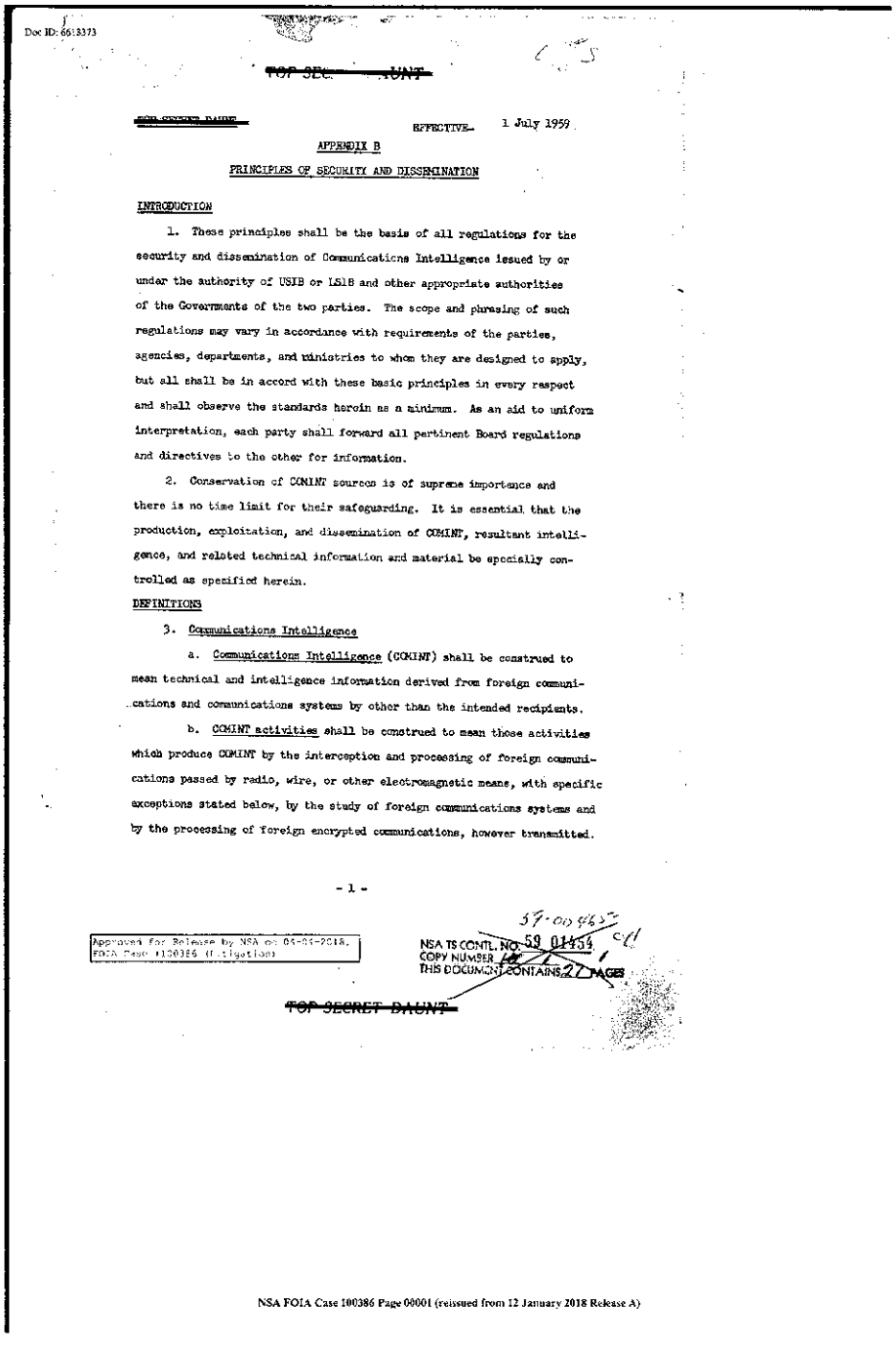
As you may be aware, the Board is currently in a sub-quorum status. While it is able to continue its ongoing projects, the Board is unable to initiate new oversight projects. Nevertheless, I appreciate hearing from you about your concerns regarding international intelligence sharing.

Thank you again for contacting me.

Sincerely,

Elisebeth Collins
Member, Privacy and Civil Liberties Oversight Board

Annex IV - Selected Disclosure from Privacy International Five Eyes Litigation



Doc ID: 6613373

~~TOP SEC[illegible] UKUSA~~

~~SECRET UMBRA~~ EFFECTIVE 1 July 1959

APPENDIX B

PRINCIPLES OF SECURITY AND DISSEMINATION

INTRODUCTION

1. These principles shall be the basis of all regulations for the security and dissemination of Communications Intelligence issued by or under the authority of USIB or LSIB and other appropriate authorities of the Governments of the two parties. The scope and phrasing of such regulations may vary in accordance with requirements of the parties, agencies, departments, and ministries to whom they are designed to apply, but all shall be in accord with these basic principles in every respect and shall observe the standards herein as a minimum. As an aid to uniform interpretation, each party shall forward all pertinent Board regulations and directives to the other for information.

2. Conservation of COMINT sources is of supreme importance and there is no time limit for their safeguarding. It is essential that the production, exploitation, and dissemination of COMINT, resultant intelligence, and related technical information and material be specially controlled as specified herein.

DEFINITIONS

3. Communications Intelligence

a. Communications Intelligence (COMINT) shall be construed to mean technical and intelligence information derived from foreign communications and communications systems by other than the intended recipients.

b. COMINT activities shall be construed to mean those activities which produce COMINT by the interception and processing of foreign communications passed by radio, wire, or other electromagnetic means, with specific exceptions stated below, by the study of foreign communications systems and by the processing of foreign encrypted communications, however transmitted.

- 1 -

Approved for Release by NSA on 04-04-2018, FOIA Case #100386 (Litigation)

NSA TS CONTL. NO. 59 01454
COPY NUMBER 4
THIS DOCUMENT CONTAINS 27 PAGES

~~TOP SECRET UMBRA~~

NSA FOIA Case 100386 Page 00001 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

Interception comprises search, intercept, and direction finding. Processing comprises range estimation, transmitter/operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain text, the fusion of these processes, and the reporting of results.

3. c. Foreign communications are defined as all communications except:

(1) Those of the Governments of the U.S. and the British Commonwealth.

(2) Those exchanged among private organizations and nationals, acting in a private capacity, of the U.S. and the British Commonwealth.

(3) Those of nationals of the U.S. and British Commonwealth appointed or seconded by their Governments to serve in international organizations.

d. COMINT concerning weather is meteorological information (hydrometeorological data and all information concerning meteorological organizations and activities) which is derived from foreign communications, except information and data which is used for recognized weather purposes and which is derived from those portions of broadcasts (the schedules of which have been published by the World Meteorological Organization (WMO) or made internationally available by a recognized civil weather organization) which contain:

(1) unenciphered WMO codes or

(2) no code or cipher or disguised indicatives or

(3) weather codes which have been made internationally available by recognized civil weather organizations.

e. Special weather intelligence is that COMINT concerning weather which is assigned to the weather sub-category of Category II. The purpose of this sub-category is to handle separately that COMINT concerning weather which may be disseminated to users who do not require access to other codeword COMINT.

59-00465 cy #1
59-01455
NSA STAFF CTL. NO.
COPY NO. 10
THIS DOCUMENT CONTAINS 27 PAGES

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00002 (reissued from 12 January 2018 Release A)

Doc ID: 66:3373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

3. f. 'Y' is tactical COMINT produced by units which are designated to provide close support for the commanders of combat forces. (See Appendix P.)

g. COMINT and COMINT activities as defined herein shall not include:

(1) Intercept and processing of unencrypted written communications, except written plain text versions of communications which have been encrypted or are intended for subsequent encryption.

(2) Intercept and processing of press, propaganda and other public broadcasts, except for encrypted or "hidden meaning" passages in such broadcasts.

(3) Certain operations conducted by U.S., U.K., or Commonwealth security authorities.

(4) Censorship.

(5) The peacetime exercise of 'Y' resources in NATO commands, which involves the interception , analysis and exploitation only of radio transmissions (albeit "foreign") on networks established or used for exercises within or between those commands, provided that:

(a) 'Y-type' information produced during the exercise or revealed in post-exercise analysis, and information about the 'Y' resources involved, is adequately safeguarded by NATO security regulations paralleling those for wartime 'Y' operations, and the U.S. and U.K. retain the right to express their views to the Command concerned as to the adequacy of the security classification applied.

(b) Techniques used in the production of exercise 'Y' during the exercise do not exceed in complexity the COMINT techniques involved in producing Category II(X) COMINT as defined in Annexure H1.

(6) The interception and study of non-communications transmissions (ELINT).

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00003 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

4. Types of COMINT

There are two types of COMINT: Crypt Intelligence and Traffic Intelligence. They are defined as follows:

a. Crypt Intelligence is that COMINT which results from cryptanalysis or decryption including the solution of speech and facsimile security systems.

b. Traffic Intelligence is that COMINT produced by all means except cryptanalysis or decryption of intercepted communications.

5. Categories

For purposes of security handling and control, COMINT is divided into categories and sub-categories. (See Annexure B1)

a. COMINT is assigned to one of the following three categories as agreed between USIB and LSIB.

(1) Category III COMINT is that COMINT the unauthorized disclosure of which would risk extremely grave damage to national interests and specifically to COMINT activities and which, therefore, requires handling under special rules affording the highest degree of security protection. It is classified TOP SECRET, and is designated by a distinctive codeword.

(2) Category II COMINT is that COMINT the unauthorized disclosure of which would risk serious damage to national interests and specifically to COMINT activities, but for which a less rigid standard of security is adequate. It is classified SECRET and is designated by a distinctive codeword.

(3) Category I COMINT is that COMINT the unauthorized disclosure of which would risk little or no damage specifically to COMINT activities and for which, therefore, normal security classification procedures may be used. It will be classified at least CONFIDENTIAL and will not be designated by a codeword.

b. As mutually agreed by USIB and LSIB, separate sub-categories of COMINT may be established within Categories III and II in order to permit

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00004 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

differentiation in the processing, dissemination, exchange or use of material.

6. Technical Material

Technical material is understood to mean data concerning:

a. Cryptographic systems.

b. Communication systems, procedures and methods.

c. Methods and equipment designed for COMINT activities and information related to any of the above.

7. Information related to COMINT or COMINT Activities - That information, other than COMINT itself, which reveals, directly or by implication, the existence or nature of any U.S. or U.K. COMINT activity.

8. COMINT Channels - A method or means expressly authorized for handling or transmission of COMINT and information related to COMINT activities whereby the information is provided exclusively to those persons who are appropriately cleared and indoctrinated for access to COMINT.

9. Codewords

Codewords, as used herein, are designators assigned to identify the source as COMINT; to distinguish between the COMINT categories and sub-categories; and to facilitate the application of regulations for the dissemination and use of COMINT.

10. Suitable Cover

Suitable cover is the concealment of any relationship between an action and the COMINT which motivates or influences the decision to take the action. It is achieved:

a. By ascribing the action to:

(1) existing intelligence from a non-COMINT source, or

(2) existing non-COMINT sources which could, beyond reasonable doubt, have produced the information leading to the action, or

b. By the existence of non-COMINT sources to which the action could be expected beyond reasonable doubt to be attributed.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00005 (reissued from 12 January 2018 Release A)

Doc ID: 6913373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

c. By the existence of a situation in which the action could be expected beyond reasonable doubt to be attributed to non-COMINT sources, or of a situation in which the action taken is so plausible that it would not be attributed to its COMINT source.

11. Proper Authority

The term "proper authority", as used herein, shall be the level of authority permitted to authorize usage of the several categories of COMINT during hostilities and in special and emergency situations. The determination to make these exceptions and the authority to grant these exceptions shall lie only with senior officers and officials at levels to be established by USIB or LSIB.

12. Indoctrination

Indoctrination is instruction as to the nature of COMINT and the security regulations and practices which govern the handling of COMINT material and COMINT activities.

13. Debriefing

Debriefing is the process of reminding persons no longer authorized to have access to COMINT or COMINT activities that they continue to be bound by all security regulations pertaining thereto. The debriefing shall include cautions that there is no time limit on the requirement to maintain security and that public disclosure does not free the individual from his obligation.

14. Hazardous Activities

Hazardous activities are those which place a person in a position where he runs a substantial risk of being captured or otherwise subjected to interrogation.

15. Exposed Areas

Exposed areas are those which are susceptible of being quickly overrun or those wherein the local political or military situation is such as to pose a distinct threat to the security of COMINT activities conducted therein.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00006 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

ASSIGNMENT OF COMINT TO CATEGORIES

16. In assigning COMINT to Categories (see paragraph 5), the following considerations will apply:

a. The difficulty of solution or intercept to include:

(1) Sensitivity of techniques employed in solution and exploitation.

(2) Sensitivity of source of intercept.

(3) Relationships to other COMINT.

b. The advantages to be gained versus the risk of disclosure and consequent damage through utilization under a given category taking into consideration the following factors:

(1) The potential loss of intelligence.

(2) The extent to which the target country is capable of improving the security of the communications in question.

(3) The security grading given to contents by the country originating the traffic involved.

(4) How wide the dissemination of certain COMINT should be to permit essential use of the intelligence contained therein.

(5) The capability of certain Third Party COMINT groups to exploit the COMINT in question with the attendant security risks beyond the direct control of U.S. and U.K. authorities.

(6) The value of providing technical guidance or COMINT information to Third Party COMINT activities to insure receipt from them of unique intercept and critical COMINT information not otherwise available.

17. USIB and LSIB shall have prepared and maintained in current status mutually agreed lists to indicate COMINT placed in the several categories and in such sub-categories as may be established.

CLASSIFICATION AND CODEWORDS

18. Separate and distinctive codewords shall be employed to designate Category III and Category II COMINT and each sub-category thereof.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00007 (released from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

Category I COMINT shall not be designated by a codeword. Codewords shall be replaced when in the opinion of either USIB or LSIB a requirement exists for a change.

19. Documents and Technical material which reveal actual or prognosticated success, progress, scale and direction of effort, or other sensitive details about the production of COMINT shall bear the classification or the classification and codeword appropriate to the highest category or sub-category of COMINT to which they relate and shall be handled accordingly, even though such documents and technical material may not contain COMINT as such.

20. Raw traffic (i.e., intercepted traffic showing no evidence of processing for COMINT purposes beyond sorting by clear address elements, elimination of unwanted messages and the inclusion of a case number and/or an arbitrary traffic designator) shall be classified not lower than CONFIDENTIAL, and is understood not to be any specific category of COMINT and need not be designated by a codeword.

21. Codewords. The fact that codewords are used to designate COMINT categories shall not be made known to non-indoctrinated persons nor shall these codewords be used in the presence of non-indoctrinated persons.

SECURITY

22. All persons, including intercept operators, to be assigned to duties involving categories of COMINT other than Category I shall be indoctrinated. Recipients of Category I COMINT only will not be indoctrinated. Producers of Category I COMINT only need not be indoctrinated.

23. Every effort shall be made to restrict the number of persons indoctrinated for COMINT to the essential minimum.

24. It shall be permissible for persons who have access only to a lower category or sub-category of COMINT to work within Agencies or Centers in which there are located other persons engaged in the production or exploitation of a higher category or sub-category of COMINT, only so

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00008 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

long as due precaution shall be taken (by providing segregated, secure areas or otherwise) to ensure that the activities and knowledge of such persons are confined to the COMINT material and activities to which they are authorized to have access.

25. Except as determined by USIB or LSIB, all persons to be assigned to duties involving COMINT shall be the subject of security investigation and clearance. As an aid to promoting uniform minimum standards of eligibility, each party shall inform the other of the standards prescribed by it for this purpose.

26. Under extraordinary conditions, as determined by USIB or LSIB, it may be essential for an individual to take up duties involving COMINT before the requisite investigation can be completed. In such cases, the person concerned may be suitably indoctrinated on the authority only of senior officers or officials as designated by the respective parties. In all such cases, steps shall be taken to ensure that security investigations and clearances are completed as soon as possible after indoctrination.

27. All persons who have been indoctrinated for COMINT shall be debriefed when they no longer have the requisite need-to-know.

28. Each party shall ensure that complete lists of indoctrinated persons are maintained.

29. USIB and LSIB shall keep each other fully informed of the approximate number of indoctrinated persons in each of the departments, ministries, agencies, and offices receiving COMINT, by category or sub-category where applicable.

30. No national of one party shall be permitted access to the COMINT organizations or to the Categories III and II COMINT of the other party, unless he has been approved by his parent organization or Board and has been properly indoctrinated. Such access shall be limited to the categories or sub-categories of COMINT agreed by his parent organization or Board.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00009 (reissued from 12 January 2018 Release A)

Doc ID: 6513373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

Annex B

31. Every effort shall be made to ensure that no person who has a knowledge of current value about COMINT, except recipients of Category I only, such that his capture or interrogation could be a substantial risk to the security of COMINT, shall be assigned to or engage in hazardous activities. All possible action shall be taken to discourage or prevent any individual with a knowledge of current value about COMINT, except recipients of Category I only, from engaging in hazardous activities in any unofficial capacity at any time. Security principles governing participation in hazardous activities are set forth in Annexure B2.

32. Collection, processing, and dissemination of COMINT in exposed areas shall be undertaken only after a careful evaluation of the advantages to be gained and the risk to the security of COMINT. Security principles governing the conduct of COMINT activities in exposed areas are set forth in Annexure B2.

33. Except as implicitly involved in the operation of paragraphs 34-37, and 39 below, codeword material shall remain exclusively in the custody of indoctrinated persons, secure from examination by non-indoctrinated persons.

DISSEMINATION AND USE OF COMINT

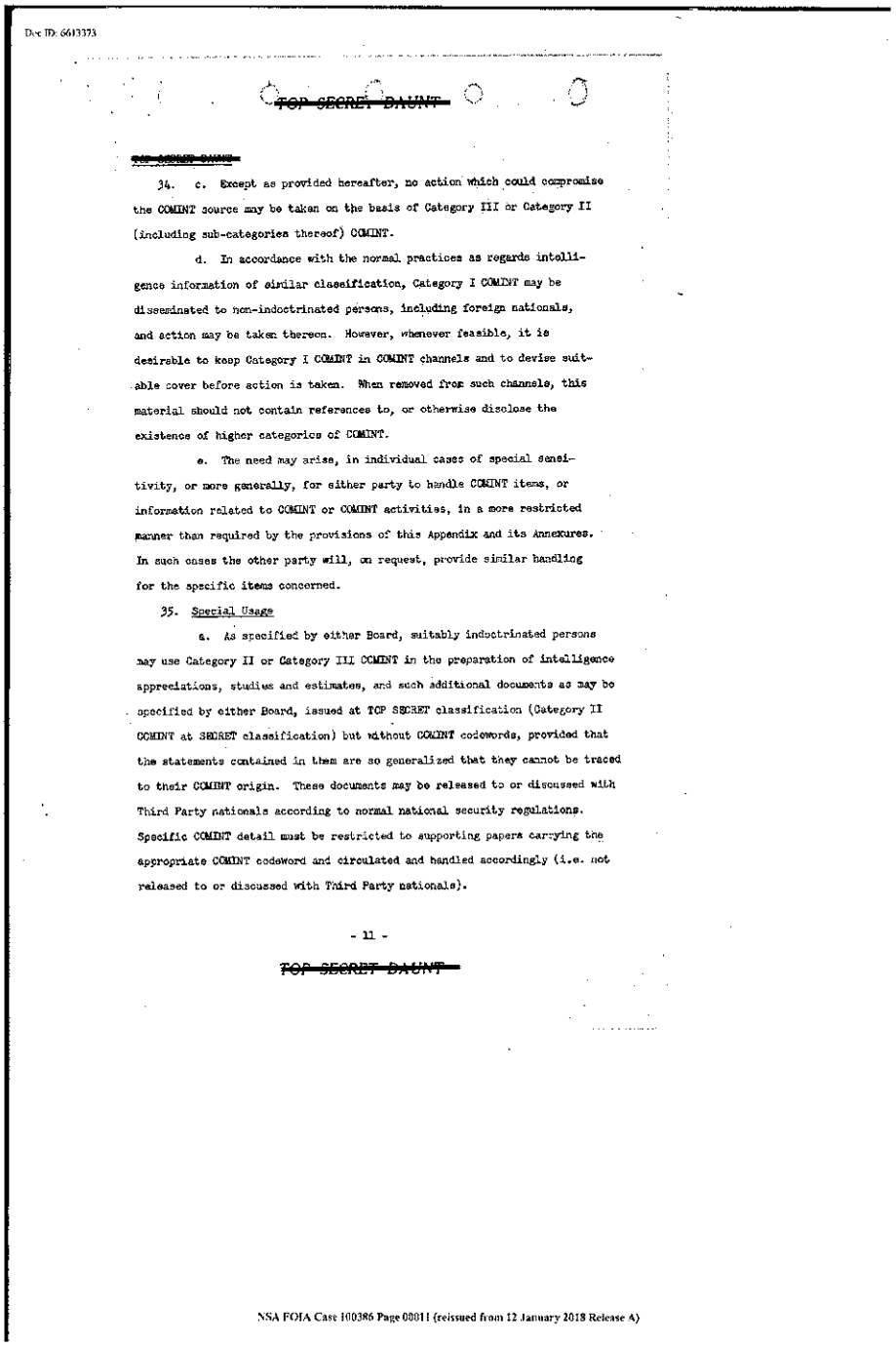
34. General

a. The basic principle governing the dissemination of COMINT is the "need-to-know". Each item of COMINT shall, therefore, be made known only to those individuals who require it in the performance of their duties.

b. Except as specifically provided in paragraphs 34d and 35-37 below each item of COMINT shall be made known only to persons who are indoctrinated and authorized to have access to the particular category or sub-category of COMINT to which such item appertains. Such persons may include nationals of collaborating British Commonwealth countries (Canada, Australia and New Zealand).

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00010 (reissued from 12 January 2018 Release A)



Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

34. c. Except as provided hereafter, no action which could compromise the COMINT source may be taken on the basis of Category III or Category II (including sub-categories thereof) COMINT.

d. In accordance with the normal practices as regards intelligence information of similar classification, Category I COMINT may be disseminated to non-indoctrinated persons, including foreign nationals, and action may be taken thereon. However, whenever feasible, it is desirable to keep Category I COMINT in COMINT channels and to devise suitable cover before action is taken. When removed from such channels, this material should not contain references to, or otherwise disclose the existence of higher categories of COMINT.

e. The need may arise, in individual cases of special sensitivity, or more generally, for either party to handle COMINT items, or information related to COMINT or COMINT activities, in a more restricted manner than required by the provisions of this Appendix and its Annexures. In such cases the other party will, on request, provide similar handling for the specific items concerned.

35. Special Usage

a. As specified by either Board, suitably indoctrinated persons may use Category II or Category III COMINT in the preparation of intelligence appreciations, studies and estimates, and such additional documents as may be specified by either Board, issued at TOP SECRET classification (Category II COMINT at SECRET classification) but without COMINT codewords, provided that the statements contained in them are so generalized that they cannot be traced to their COMINT origin. These documents may be released to or discussed with Third Party nationals according to normal national security regulations. Specific COMINT detail must be restricted to supporting papers carrying the appropriate COMINT codeword and circulated and handled accordingly (i.e. not released to or discussed with Third Party nationals).

- 11 -

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00011 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

35. b. As specified by either Board, information derived from Category II or Category III COMINT, for which there is suitable cover, may be entered without the COMINT codeword in the following types of classified documents: departmental and theater plans, maps, and target folders, but only in such form as does not indicate or reveal the COMINT origin.

c. Upon determination by proper authority that suitable cover exists and that the advantage to be gained clearly outweighs the possible risk of loss of the COMINT source and consequently of valuable intelligence, action may be taken on the basis of Category II or Category III COMINT. In determining the "proper authority" for this paragraph (see paragraph 11) particular attention will be paid to the need for the authority to be such that the consequences of the possible loss of the COMINT source will be taken

[redacted]

d. As specified by either Board, technical instructions based upon Category II or Category III COMINT may be issued to non-indoctrinated intercept operators (including D/F, RFP operators, and the like) without use of the appropriate codeword, if in such form and of such nature as to give no indication of the specific COMINT origin, and provided they are essential to the tasks of those concerned.

e. Category II or Category III COMINT material, exclusive of end product, may be handled by indoctrinated persons within COMINT collection or processing agencies without the use of the appropriate codeword.

f. As specified by either Board, weather forecasts or conclusions based in whole or in part on analysis of maps, etc., on which Special Weather Intelligence material has been plotted, may be issued to non-indoctrinated persons who require such information in the performance of their duties,

NSA FOIA Case I00386 Page 00012 (released from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

provided the form of issue gives no indication whatever of the COMINT origin.

35. g. Certain less sensitive Category II COMINT designated by USIB and LSIB may be assigned to a sub-category to permit more effective utilization (see paragraph 5b of Annexure B1). Upon determination by proper authority that it is in the national interest, or necessary for the protection of armed forces, action, without cover, may be taken on this material and it may be included in non-codeword documents, and it may be disseminated without codeword to non-indoctrinated persons, including foreign nationals, provided: (1) that the material is classified at least SECRET; (2) that direct evidence of the specific COMINT source -- communication data such as frequencies, callsigns, network identifications, etc., -- is omitted except in cases where that data is prerequisite to its use by the non-indoctrinated persons involved and (3) that as much other detail is omitted as is consistent with effective use. Whenever action is taken or dissemination made under the provisions of this paragraph, NSA and GCHQ, through technical channels, will undertake to keep the other party informed, at least in general terms, of the material involved.

h. When required for 'Y' planning purposes the U.S. and U.K. national 'Y' authorities may furnish technical material to the level of the sub-category mentioned in paragraph g above to SACEUR and SACLANT for provision on a need-to-know basis to Third Party nationals in SACEUR and SACLANT commands. Such material will not carry a COMINT codeword.

i. Sub-paragraph 34d above applies with respect to special usage of Category I COMINT.

36. Emergency

a. In an extreme emergency Category III COMINT may be disseminated to non-indoctrinated persons, including foreign nationals, and action without cover may be taken, based solely on that COMINT, provided that proper authority has determined that such utilization is necessary to counter an imminent threat to vital national interests.

b. In an emergency Category II COMINT, including Special Weather Intelligence, may be disseminated to non-indoctrinated persons, including foreign nationals, and action without cover may be taken based solely on that

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00013 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

COMINT, provided that proper authority has determined that such utilization is necessary to the national security or, in the case of a military commander, to the security of forces under his command.

36. c. The decision to execute the provisions of paragraphs a and b above shall be made only after a determination that the advantages to be gained clearly juntify the risk of compromise of the source. Due regard shall also be given to:

(1) The relative value of the particular COMINT source involved and the possibility that its compromise may lead to the loss of other COMINT sources.

(2) The possible repercussions on current and future operations and also on other commands and areas.

d. In order to minimize the risk of compromise the following precautions shall be observed:

(1) A studied effort shall be made to insure, insofar as possible, that the action taken cannot be attributed to information obtained from a COMINT source. Suitable cover, if not available, shall be arranged (e.g. air reconnaissance) if time permits.

(2) A minimum number of non-indoctrinated personnel shall be given the information, and

(a) when practicable the information shall be so presented that it cannot be traced to COMINT as a source, or

(b) if it is necessary to cite COMINT as the source in order to validate the information, the specific COMINT source shall be revealed only when absolutely necessary.

(3) The minimum amount of information necessary to justify the contemplated action shall be revealed.

e. If communications by electrical means are involved they must be enciphered in the most secure cryptographic system available.

f. If time permits the commander or official making this decision should consult with his supporting COMINT authority for technical advice.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00014 (reissued from 12 January 2018 Release A)

Doc ID: 66 3373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

36. g. Whenever any of the provisions of sub-paragraphs 36a or 36b, above, are executed, USIB and LSIB will keep each other informed. This information shall contain a description of the COMINT material involved, and, in general terms, the extent and nature of the action taken. If Third Parties are involved USIB and LSIB will consult beforehand if time allows.

h. Sub-paragraph 35g above, applies with respect to emergency usage of the material in the sub-category of Category II described therein.

i. Sub-paragraph 34d, above, applies with respect to emergency usage of Category I COMINT.

37. Hostilities

a. It is recognized that in the event of hostilities certain material will be downgraded. In connection with the mutually agreed lists referred to in paragraph 17, USIB and LSIB will agree upon types of materials suitable for downgrading during hostilities. When hostilities appear imminent or occur the two Boards will immediately consult upon downgrading measures to be taken.

b. Category III COMINT designated by USIB and LSIB as "conditionally releasable COMINT" may be disseminated to non-indoctrinated persons in NATO commands, including foreign nationals. The conditions specified in Appendix P must be observed.

c. Category II COMINT may be disseminated to 'F'-indoctrinated persons in NATO commands in accordance with special security regulations in Appendix P provided it is not expressly excluded by USIB and LSIB.

d. In an extreme emergency Category III COMINT may be disseminated to non-indoctrinated persons, including foreign nationals, and action without cover may be taken, based solely on that COMINT, provided that proper authority has determined that such utilization is vital to the successful prosecution of the war. Prior to invoking this provision, due consideration shall be given to the conditions described in sub-paragraphs 36c-36f.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00015 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

37. e. In an emergency Category II COMINT may be disseminated to non-indoctrinated persons, including foreign nationals, and action without cover may be taken, based solely on that COMINT, provided the proper authority has determined that such utilization is necessary to the national security or, in the case of a military commander, to the security of forces under his command. Prior to invoking this provision, due consideration shall be given to the conditions described in sub-paragraphs 36e-36f.

f. Whenever any of the provisions of sub-paragraphs 37d and 37e, above, are executed, USIB and LSIB will keep each other informed. This information shall contain a description of the COMINT material involved, and, in general terms, the extent and nature of the action taken.

g. In the event of hostilities the proper authority may direct the appropriate COMINT organization responsible for providing his support to downgrade to Category I that material in the sub-category of Category II described in paragraph 35g which is relevant to the situation. Such information may then be disseminated or action be taken thereon in accordance with the procedures established for Category I COMINT. The cognizant COMINT organization will immediately, without prior consultation with higher authority, make available as Category I such material of this sub-category as is required. USIB and LSIB will keep each other informed of downgrading actions taken.

h. Sub-paragraph 34d, above, applies with respect to wartime usage of Category I COMINT. Whenever suitable 'Y' channels are available, they will be used for this dissemination.

PROCEDURES

38. The appropriate classification and codeword shall:

a. Appear on every sheet of paper which contains or discloses Category III or II COMINT or a sub-category thereof, and be applied to documents and technical material as defined in paragraph 19. Except as provided in paragraphs 35-37, above, this rule applies to maps and charts on which are plotted data and information derived from these categories of COMINT.

- 16 -

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00016 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~COD CODEWORD~~

38. b. Be encrypted in the text of every encrypted communication conveying Category III or II COMINT and appear in plain language at the head of the decrypted version. This rule shall apply in all instances except as provided in paragraphs 35-37, above, and under the following conditions:

(1) COMINT organizations may, without encrypting the appropriate codeword in the encrypted text, transmit TOP SECRET and SECRET technical matter over cryptographic channels or ciphers expressly and exclusively provided for such technical matters.

(2) COMINT organizations and intercept or D/F stations may, at the discretion of the officer in charge and after full consideration of the risks involved to the source, omit the classification and the appropriate codeword from its work-sheets and similar documents used exclusively within each agency or station. The classification may be omitted from raw traffic passed between agencies or from intercept and D/F stations to agencies.

39. Category III COMINT and related technical material shall not be transmitted in plain language except as follows:

a. Sealed, by safehand channels, over routes specifically approved by USIB or LSIB.

b. Over completely protected local communication systems exclusively internal to agencies or offices producing or utilizing COMINT.

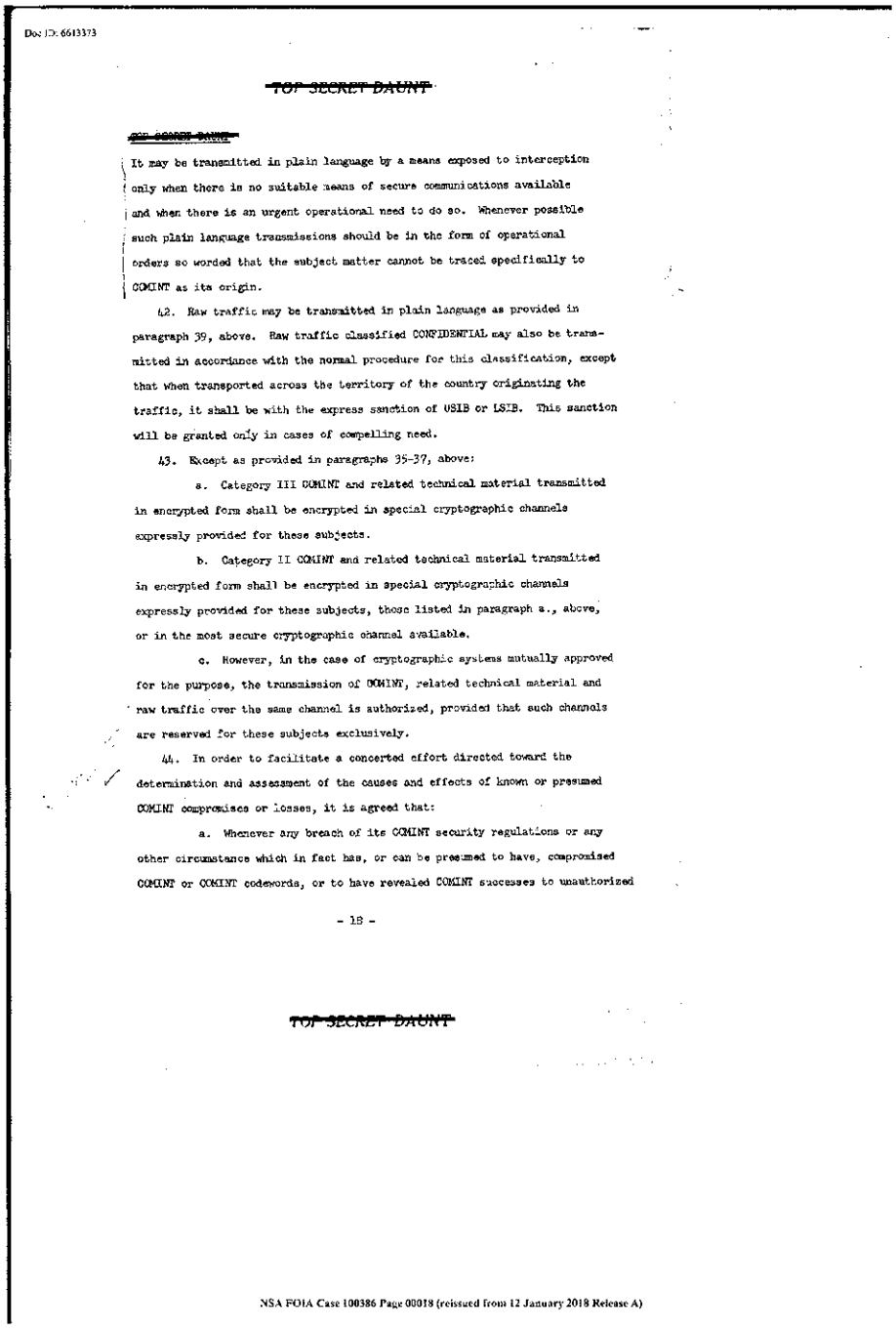
c. Over landlines specifically approved in each instance by USIB or LSIB.

40. Category II COMINT and related technical material shall not be transmitted in plain language except as provided in paragraph 39 above, or by protected postal channels internal to, or under exclusive control of, the U. S., the U. K. or other collaborating British Commonwealth countries.

41. Category I COMINT and related technical material should be transmitted by COMINT or 'Y' channels wherever possible, but may be transmitted by conventional channels used for intelligence materials of similar classification.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00017 (reissued from 12 January 2018 Release A)



Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

It may be transmitted in plain language by a means exposed to interception only when there is no suitable means of secure communications available and when there is an urgent operational need to do so. Whenever possible such plain language transmissions should be in the form of operational orders so worded that the subject matter cannot be traced specifically to COMINT as its origin.

42. Raw traffic may be transmitted in plain language as provided in paragraph 39, above. Raw traffic classified CONFIDENTIAL may also be transmitted in accordance with the normal procedure for this classification, except that when transported across the territory of the country originating the traffic, it shall be with the express sanction of USIB or LSIB. This sanction will be granted only in cases of compelling need.

43. Except as provided in paragraphs 35-37, above:

a. Category III COMINT and related technical material transmitted in encrypted form shall be encrypted in special cryptographic channels expressly provided for these subjects.

b. Category II COMINT and related technical material transmitted in encrypted form shall be encrypted in special cryptographic channels expressly provided for these subjects, those listed in paragraph a., above, or in the most secure cryptographic channel available.

c. However, in the case of cryptographic systems mutually approved for the purpose, the transmission of COMINT, related technical material and raw traffic over the same channel is authorized, provided that such channels are reserved for these subjects exclusively.

44. In order to facilitate a concerted effort directed toward the determination and assessment of the causes and effects of known or presumed COMINT compromises or losses, it is agreed that:

a. Whenever any breach of its COMINT security regulations or any other circumstance which in fact has, or can be presumed to have, compromised COMINT or COMINT codewords, or to have revealed COMINT successes to unauthorized

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00018 (reissued from 12 January 2018 Release A)

Doc ID: 6613373

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

persons, becomes known to either party, it shall inform the other by means of a report embodying the pertinent facts and conclusions in each case, except that when the party concerned concludes that there is a good reason to believe that such compromise or revelation has not reached and will not, in fact, reach foreign nationals, no report need be made to the other party.

b. Whenever a significant change occurs in foreign cryptographic or communications security, the party discovering such change shall notify the other. Each party shall then analyze and assess the known and suspected circumstances having a bearing upon the change; these analyses and assessments shall be exchanged by the parties; and each party shall thereafter keep the other fully informed of any additional information bearing upon the case.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00019 (reissued from 12 January 2018 Release A)

Doc ID: 6613432

~~TOP SECRET BAUNT~~

~~TOP SECRET BAUNT~~ 1 July 1959

APPENDIX B

ANNEXURE B1

THE ASSIGNMENT OF COMINT

TO CATEGORIES AND SUB-CATEGORIES

1. This Annexure delineates the basis for (a) the establishment of sub-categories, (b) the assignment of COMINT to categories and sub-categories, (c) the classification of COMINT assigned to categories and sub-categories, and (d) the application of codewords to categories and sub-categories. This Annexure is not intended to accomplish the detailed categorization of all COMINT. However, along with the criteria described in Appendix B, it governs the preparation and maintenance of current, mutually agreed lists to indicate the precise assignment of all COMINT to categories and sub-categories.

2. Category I COMINT shall be classified CONFIDENTIAL, SECRET, or TOP SECRET as appropriate in accordance with national security classification procedures and shall not be designated by a codeword. It shall contain the following, provided that interpretations of material of higher categories are not included:

a. Direction finding results, regardless of the category of technical guidance involved. This material shall normally be classified as CONFIDENTIAL.

b. COMINT concerning weather derived from Category I sources.

c. Such COMINT from the less sensitive sub-category of Category II as may be so assigned in accordance with Appendix B. (See paragraph 35g)

d. Such additional COMINT as has been or may be specified and mutually agreed by USIB and LSIB.

~~TOP SECRET BAUNT~~

Approved for Release by NSA on 04-04-2018, FOIA Case #100386 (Litigation)

NSA FOIA Case 100386 Page 00020 (reissued from 12 January 2018 Release A)

Doc ID: 6613432

~~TOP SECRET BAUNT~~

~~TOP SECRET BAUNT~~

3. Category II COMINT shall be classified SECRET and shall be designated by a distinctive codeword. It shall contain all COMINT not otherwise assigned to Categories I and III, or sub-categories within Category II.

4. Category III COMINT shall be classified TOP SECRET, and shall be designated by a distinctive codeword. It shall contain:

a. Crypt Intelligence derived from high-grade systems, involving the application of sophisticated cryptanalytic techniques, as specified and mutually agreed by USIB and LSIB.

b. Traffic Intelligence derived from callsigns or message headings encrypted in codes and ciphers of high security or complexity, as specified and mutually agreed by USIB and LSIB.

c. Traffic or Crypt Intelligence which reveals success against unusual, sensitive, or complex transmission procedures or devices.

d. Material obtained from special sources or against targets considered by the procuring organization to be so sensitive as to warrant the protection afforded this category.

e. Crypt Intelligence from diplomatic and attaché communications.

f. Other Crypt or Traffic Intelligence which USIB and LSIB agree should be given the highest degree of security protection because of the potential loss of intelligence which would result from compromise.

5. Sub-categories of Category II shall be established as follows:

a. Sub-Category II(W) COMINT shall contain all COMINT concerning weather, which is not specifically assigned to other categories by USIB and LSIB. It is classified SECRET, designated by a distinctive codeword, and referred to as "Special Weather Intelligence". The purpose of this sub-category is to handle separately that COMINT concerning weather which may be disseminated to users who do not require access to other codeword COMINT.

~~TOP SECRET BAUNT~~

NSA FOIA Case 100386 Page 00021 (reissued from 12 January 2018 Release A)

Doc ID: 6613432

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

b. Sub-Category II(X) COMINT is that Category II COMINT which is considered less sensitive than other Category II COMINT and may, therefore, be given more extensive dissemination in order to provide for effective utilization. It is classified SECRET and is designated by a distinctive codeword. It is this sub-category which is described in paragraph 35g of Appendix B. Provided that no information obtained from Categories II and III COMINT, such as complex changing callsign and frequency systems or unusual, sensitive or complex transmission procedures or devices, is included, this sub-category shall contain the following:

(1) Information derived from the following elements of foreign military, naval, air, police, border guard and guerilla communications or communications systems:

(a) Communications data

(b) Plain Text

(c) Any grid or zone references

(d) Cover Words

(e) Procedural codes used for brevity purposes

(f) Jargon codes

(2) Plain Text and associated communications data obtained from international commercial and foreign internal or external non-military circuits except that specifically assigned to other categories as mutually agreed by USIB and LSIB.

(3) Such additional COMINT as may be specified and mutually agreed by USIB and LSIB.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00022 (reissued from 12 January 2018 Release A)

Doc ID: 6613058

~~TOP SECRET BAUNT~~

~~TOP SECRET BAUNT~~ 21 March 1960

APPENDIX B

ANNEXURE B2

SECURITY PRINCIPLES GOVERNING THE CONDUCT

OF COMINT OPERATIONS IN EXPOSED AREAS

INTRODUCTION

1. It is recognized that effective interception of foreign communications and effective support of field commanders may require the establishment of COMINT activities in locations which may suddenly fall under hostile control with consequent loss of COMINT personnel and/or associated classified materials. It is agreed that, in addition to the pertinent, general provisions of Appendix B, the specific provisions which follow shall govern the conduct of COMINT activities in such locations.

DEFINITIONS

2. Exposed areas as defined in paragraph 15, Appendix B comprise the Sino-Soviet Bloc, other countries under bloc domination, areas beyond defense lines expected to be tenable, and areas wherein the local political or military situation is such as to pose a distinct threat to the security of COMINT operations conducted therein. The degree of risk is dependent upon the capability of support and security forces to protect the COMINT unit through sufficient delaying action to allow time for the destruction of classified material and prompt evacuation of COMINT personnel. The following situations may exist in exposed areas:

a. Risky situations, i.e., those in which it is considered possible that timely and complete evacuation of COMINT personnel and removal or effective destruction of classified material will be accomplished before a unit can be overrun.

b. Dangerous situations, i.e., those in which it is unlikely that timely and complete evacuation of COMINT personnel and removal or

Approved for Release by NSA on 04-04-2018, FOIA Case #100386 (litigation)

59-00465

NSA TS CONTROL NO. 8-1174

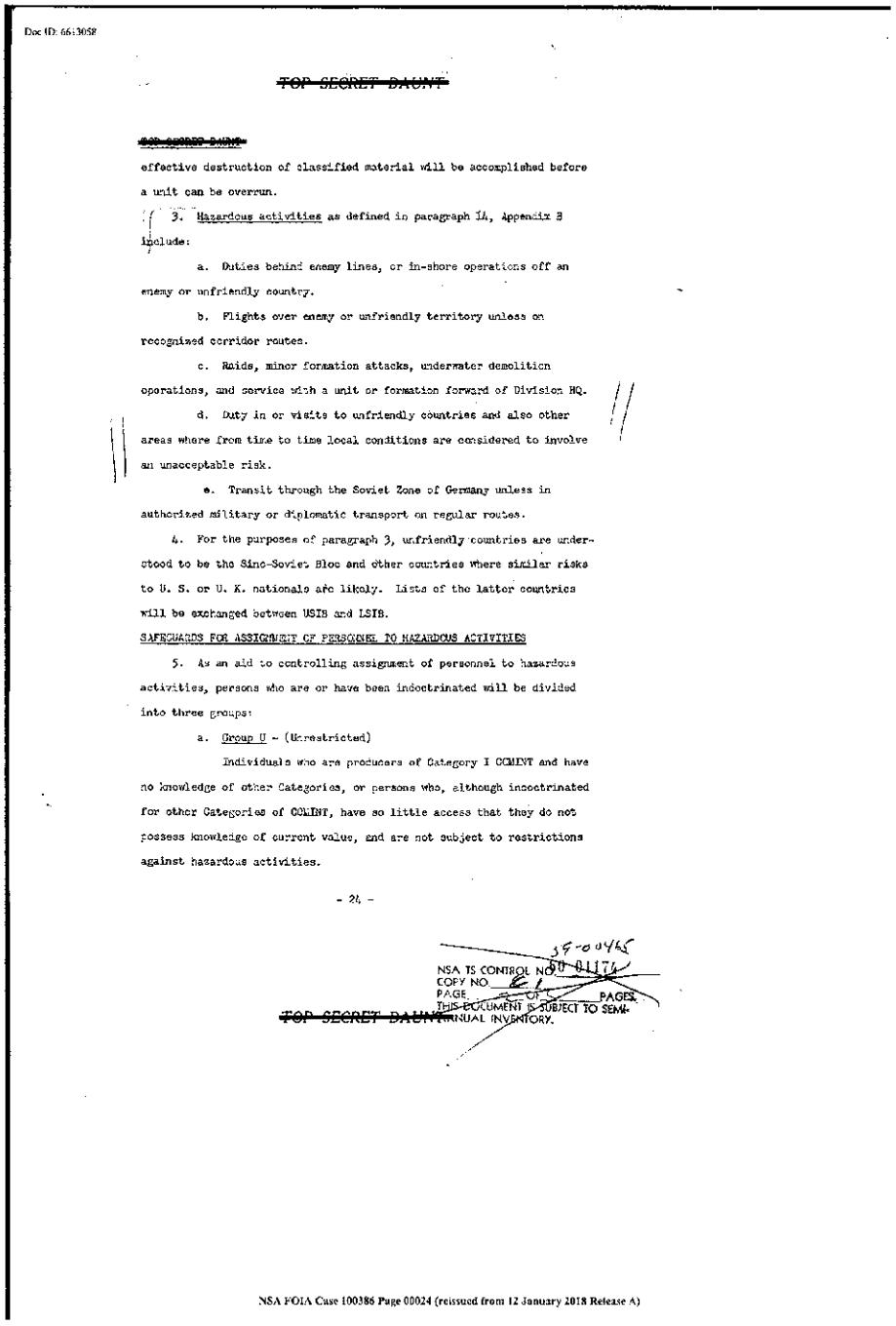
COPY NO. 1

PAGE 1 OF 5 PAGES

THIS DOCUMENT IS SUBJECT TO SEMI-ANNUAL INVENTORY.

~~TOP SECRET BAUNT~~

NSA FOIA Case 100386 Page 00023 (reissued from 12 January 2018 Release A)



Doc ID: 6613058

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

effective destruction of classified material will be accomplished before a unit can be overrun.

3. Hazardous activities as defined in paragraph 1A, Appendix B include:

a. Duties behind enemy lines, or in-shore operations off an enemy or unfriendly country.

b. Flights over enemy or unfriendly territory unless on recognized corridor routes.

c. Raids, minor formation attacks, underwater demolition operations, and service with a unit or formation forward of Division HQ.

d. Duty in or visits to unfriendly countries and also other areas where from time to time local conditions are considered to involve an unacceptable risk.

e. Transit through the Soviet Zone of Germany unless in authorized military or diplomatic transport on regular routes.

4. For the purposes of paragraph 3, unfriendly countries are understood to be the Sino-Soviet Bloc and other countries where similar risks to U. S. or U. K. nationals are likely. Lists of the latter countries will be exchanged between USIB and LSIB.

SAFEGUARDS FOR ASSIGNMENT OF PERSONNEL TO HAZARDOUS ACTIVITIES

5. As an aid to controlling assignment of personnel to hazardous activities, persons who are or have been indoctrinated will be divided into three groups:

a. Group U - (Unrestricted)

Individuals who are producers of Category I COMINT and have no knowledge of other Categories, or persons who, although indoctrinated for other Categories of COMINT, have so little access that they do not possess knowledge of current value, and are not subject to restrictions against hazardous activities.

- 24 -

NSA TS CONTROL NO 55-00445
COPY NO 61
PAGE 1 OF 1 PAGES
THIS DOCUMENT IS SUBJECT TO SEMI-ANNUAL INVENTORY.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00024 (reissued from 12 January 2018 Release A)

Doc ID: 6613058

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

b. Group M - (Minimum Restriction - one year)

Individuals who have knowledge of current value about Categories II or III COMINT or their subcategories, who shall not be assigned to hazardous activities for a minimum period of one year following debriefing.

c. Group P - (Permanent Restriction)

Individuals with precise knowledge of COMINT processing techniques, competence or potential regarding the more sensitive Category III COMINT who shall not be assigned to hazardous activities at any time.

6. Exceptions to the above safeguards may be authorized by senior officers and officials at a level prescribed by USIB or LSIB. In considering such exceptions the protection offered by diplomatic status should not automatically be considered sufficient, but should be assessed in the light of the particular circumstances involved. In the case of Allied Commands to which UKUSA COMINT is provided through an SSO or CCU, the senior COMINT indoctrinated U. S. and U. K. officers shall be authorized to make such exceptions.

EVALUATION OF SITUATIONS IN EXPOSED AREAS

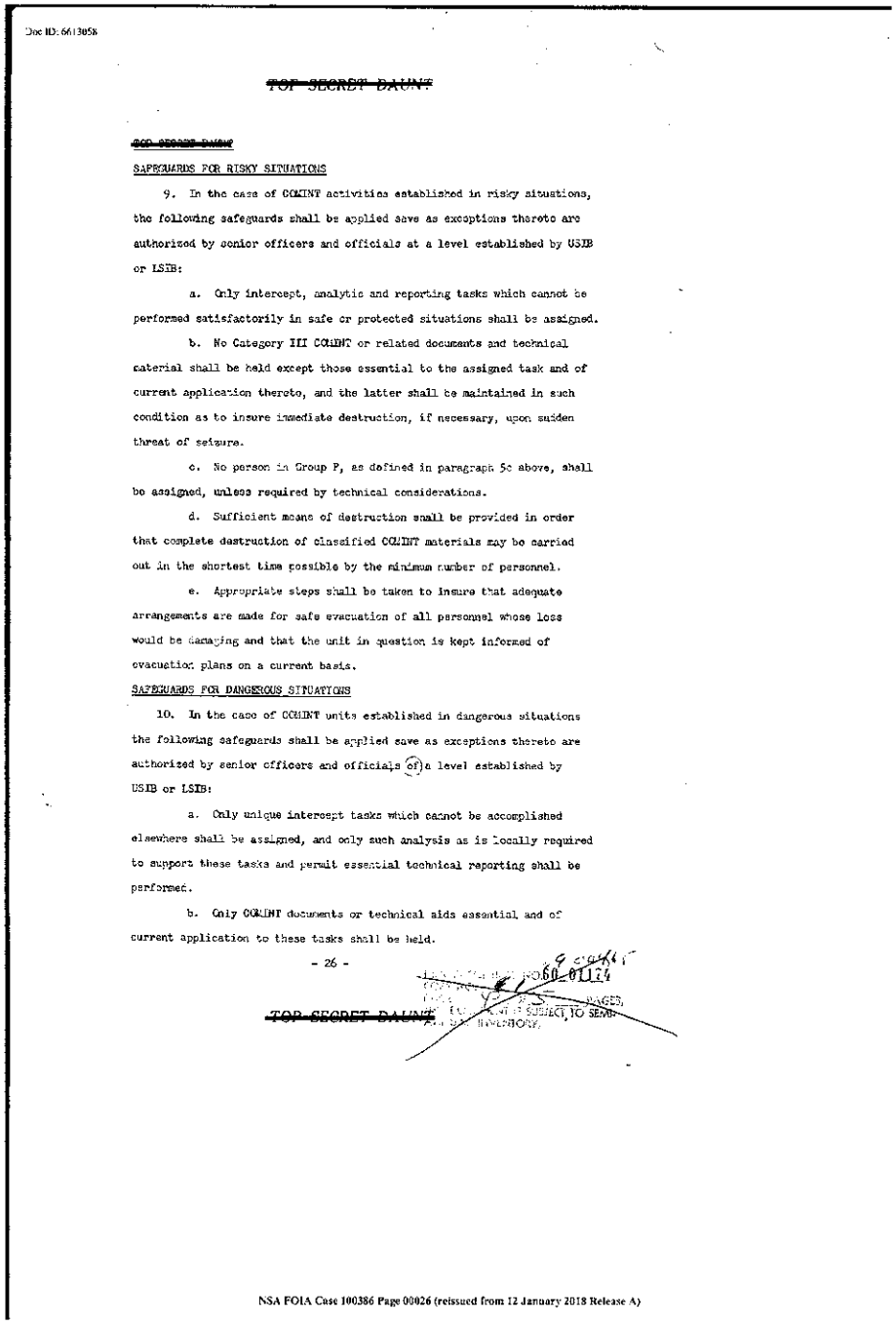
7. The decision whether a given situation is risky or dangerous shall be made by USIB or LSIB or by such other authorities as are responsible for the security of the COMINT activities concerned, and shall be made in the light of the political, military, and other factors affecting the safety of the COMINT personnel and materials involved.

FACTORS AFFECTING DECISIONS TO CONDUCT COMINT OPERATIONS IN EXPOSED AREAS

8. COMINT operations shall be conducted in exposed areas only after due consideration of the COMINT losses which may result if the area concerned is suddenly attacked, and of the probable effect of such losses upon the conduct of COMINT activities elsewhere.

NSA TS CONTROL NO. 60-01174 cy 1
COPY NO.
PAGE 2 OF 3 PAGES
THIS DOCUMENT CONSISTS OF [illegible] SERIES A
~~TOP SECRET DAUNT~~ [illegible]

NSA FOIA Case 100386 Page 00025 (reissued from 12 January 2018 Release A)



Doc ID: 6613058

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

SAFEGUARDS FOR RISKY SITUATIONS

9. In the case of COMINT activities established in risky situations, the following safeguards shall be applied save as exceptions thereto are authorized by senior officers and officials at a level established by USIB or LSIB:

a. Only intercept, analytic and reporting tasks which cannot be performed satisfactorily in safe or protected situations shall be assigned.

b. No Category III COMINT or related documents and technical material shall be held except those essential to the assigned task and of current application thereto, and the latter shall be maintained in such condition as to insure immediate destruction, if necessary, upon sudden threat of seizure.

c. No person in Group P, as defined in paragraph 5c above, shall be assigned, unless required by technical considerations.

d. Sufficient means of destruction shall be provided in order that complete destruction of classified COMINT materials may be carried out in the shortest time possible by the minimum number of personnel.

e. Appropriate steps shall be taken to insure that adequate arrangements are made for safe evacuation of all personnel whose loss would be damaging and that the unit in question is kept informed of evacuation plans on a current basis.

SAFEGUARDS FOR DANGEROUS SITUATIONS

10. In the case of COMINT units established in dangerous situations the following safeguards shall be applied save as exceptions thereto are authorized by senior officers and officials of a level established by USIB or LSIB:

a. Only unique intercept tasks which cannot be accomplished elsewhere shall be assigned, and only such analysis as is locally required to support these tasks and permit essential technical reporting shall be performed.

b. Only COMINT documents or technical aids essential and of current application to these tasks shall be held.

- 26 -

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00026 (reissued from 12 January 2018 Release A)

Doc ID: 6613058

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

c. No Category III COMINT or related documents and technical material shall be held.

d. Personnel technically informed in COMINT of a higher level or broader scope than is required for the limited mission of the unit should not be assigned if avoidable.

e. No person in Group M as defined in sub-paragraph 5b above shall be assigned unless his presence is vital for the effective functioning of the unit.

f. No person in Group P as defined in sub-paragraph 5c above shall be assigned in any circumstances.

g. Sufficient means of destruction shall be provided in order that maximum destruction of classified COMINT material may be carried out in the shortest time possible by the minimum number of personnel.

h. Appropriate steps shall be taken to insure that the unit in question is kept informed of evacuation plans on a current basis.

- 27 -

60 01174

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00027 (reissued from 12 January 2018 Release A)

Doc ID: 6613069

TOP SECRET ~~DINAR~~

13 FEB 1961

APPENDIX J

PRINCIPLES OF UKUSA COLLABORATION WITH COMMONWEALTH COUNTRIES OTHER THAN THE UK

Introduction

1. This Appendix records the general principles governing UKUSA COMINT collaboration with Commonwealth countries (other than the UK).

General

2. Commonwealth countries other than the UK are not parties to the UKUSA COMINT Agreement but they will not be regarded as Third Parties. Canada, Australia and New Zealand with whom there are special agreements on COMINT policy are referred to as collaborating countries.

3. LSIB will keep USIB informed of any arrangements or proposed arrangements with Commonwealth countries and will obtain the views of USIB prior to initiating or pursuing with any non-collaborating country COMINT arrangements involving the release of material or the provision of guidance in accordance with paragraph 9 of Appendix P. Prior to the release to a non-collaborating country of data as described in sub-paragraph 8(e) of Appendix P, GCHQ will obtain the view of NSA regarding the suitability of the data for release.

4. Arrangements for collaboration between the U.S. and the joint Australian/UK/New Zealand agency, Defence Signals Branch Melbourne, and for U.S. liaison in Australia and New Zealand are set out in Annexure J1. Any major changes in or additions to these arrangements for U.S. collaboration with Australia and New Zealand will be the subject of prior consultation between USIB and LSIB.

5. USIB will obtain the views of LSIB prior to completing an arrangement with Canada.

6. USIB will conduct its arrangements with all other Commonwealth countries in accordance with the principles set out in Appendix P to the UKUSA COMINT Agreement.

7. It is noted that LSIB has obtained from the COMINT authorities of collaborating Commonwealth countries formal assurances that they will abide by the terms of paragraphs 5, 8, and 9 of the UKUSA COMINT Agreement, and of Appendix B and paragraph 7 of Appendix E thereto.

Approved for Release by NSA on 04-04-2014, FOIA Case #100386 (litigation)

59-00465

NSA TS CONTROL NO. 61 00471
COPY NO. 25
PAGE 1 OF 4 PAGES
THIS DOCUMENT IS SUBJECT TO SEMI-ANNUAL INVENTORY.

TOP SECRET ~~DINAR~~

NSA FOIA Case 100386 Page 00028 (reissued from 12 January 2018 Release A)

Doc ID: 6613060

~~TOP SECRET PINAR~~

8. USIB and LSIB agree:

(a) not to pass to any Commonwealth country COMINT end-product items originated by agencies of the other party without the consent of that party, except as may be agreed from time to time;

(b) to pass to collaborating Commonwealth countries, via agreed COMINT channels, only such technical COMINT materials as are deemed to be relevant to the tasks of the Commonwealth country concerned or as may be otherwise agreed between the two parties from time to time; the relevance of technical COMINT materials to the tasks of those Commonwealth countries shall be determined by the Director, GCHQ or the Director, NSA; relevant materials shall then be releasable subject to whatever restrictions may be specified by the agency which produced the material (i.e. GCHQ or NSA).

59-00465

NSA TS CONTROL NO. 61 10041
COPY NO. 26 OF 4 PAGES
~~TOP SECRET PINAR~~ THIS DOCUMENT IS SUBJECT TO SEMI-ANNUAL INVENTORY.

NSA FOIA Case 100386 Page 00029 (reissued from 12 January 2018 Release A)

Doc ID: 6613062

~~TOP SECRET DINAR~~

APPENDIX J

ANNEXURE J1

UKUSA ARRANGEMENTS AFFECTING AUSTRALIA AND NEW ZEALAND

1. It is noted that Defence Signals Branch Melbourne (DSB) is, in contrast to Communications Branch Ottawa, not a purely national centre. It is and will continue to be a joint UK-Australian-New Zealand organization, manned by an integrated staff. It is a civilian organization under the Australian Department of Defence and undertakes COMINT tasks as agreed between the COMINT governing authorities of Australia and New Zealand on the one hand and LSIB on the other. On technical matters only, control is exercised by Government Communications Headquarters on behalf of LSIB.

2. GCHQ will keep NSA informed of the tasks that have been agreed for DSB and will notify NSA in advance before any new or altered task is agreed for DSB.

3. NSA and DSB will collaborate directly on those DSB tasks which, as determined by NSA, fall within the field of collaboration and will exchange raw material, technical material and end-product of these tasks. In addition NSA will provide DSB with raw material, technical material and end-product as appropriate on other tasks determined by NSA to be relevant to the tasks of DSB. A list of tasks under both these heads will be maintained currently by NSA and GCHQ.

4. NSA and DSB will also exchange technical interception data relating to the General Search effort of each in the Far East.

5. Exchanges between NSA and DSB under the above paragraphs will be complete in scope but in special circumstances each agency will have the right to withhold material at its discretion.

6. The direct collaboration and consequent exchanges between NSA and DSB will be regulated by the provisions of the following appendices to the UKUSA Agreement: C, D, E, F, G, H, I, L, M.

7. It is noted that, in interpretation of Appendix I to the UKUSA Agreement, LSB and NSA have mutually accredited liaison officers.

8. It is further noted that, in interpretation of Appendix I to the

59-00465

Cy #1

Approved for Release by NSA on 04-24-2018, FOIA Case #100386 (Litigation)

NSA IS CONTROL NO. 61 00571
COPY NO. 4
PAGE 3 OF 5 PAGES.
THIS DOCUMENT IS SUBJECT TO SEMI-ANNUAL INVENTORY.

~~TOP SECRET DINAR~~

NSA FOIA Case 100386 Page 00030 (reissued from 12 January 2018 Release A)

Doc ID: 6613052

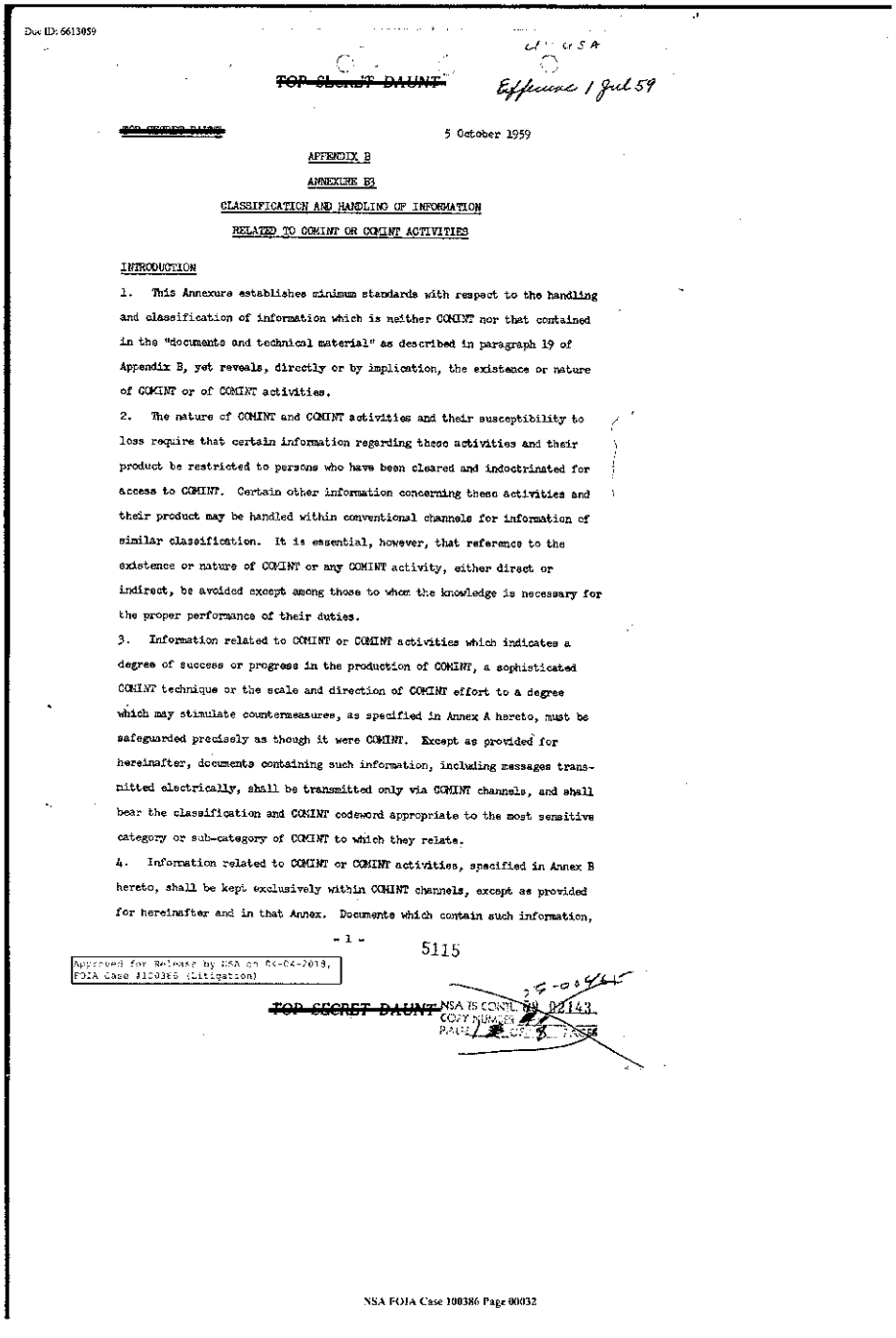
~~TOP SECRET DINAR~~

UKUSA Agreement, USIB may accredit a senior U.S. representative for conducting liaison on matters pertaining to COMINT with Australia and New Zealand and, as may be agreed by LSIB, with UK officials in those countries. Similarly, the terms of reference for the DSB liaison officer accredited to NSA may be modified at some future date to permit the conduct of liaison with U.S. authorities on matters pertaining to COMINT.

59-0045
Cy #1

NSA TS CONTROL NO. 61-00471
COPY NO. 26
PAGE 1 OF 1 PAGES.
~~TOP SECRET DINAR~~ THIS DOCUMENT IS SUBJECT TO SEMI-ANNUAL INVENTORY.

NSA FOIA Case 100386 Page 00031 (reissued from 12 January 2018 Release A)



Doc ID: 6613059

~~TOP SECRET DAUNT~~

Effective 1 Jul 59

~~TOP SECRET DAUNT~~

5 October 1959

APPENDIX B

ANNEXURE B3

CLASSIFICATION AND HANDLING OF INFORMATION

RELATED TO COMINT OR COMINT ACTIVITIES

INTRODUCTION

1. This Annexure establishes minimum standards with respect to the handling and classification of information which is neither COMINT nor that contained in the "documents and technical material" as described in paragraph 19 of Appendix B, yet reveals, directly or by implication, the existence or nature of COMINT or of COMINT activities.

2. The nature of COMINT and COMINT activities and their susceptibility to loss require that certain information regarding these activities and their product be restricted to persons who have been cleared and indoctrinated for access to COMINT. Certain other information concerning these activities and their product may be handled within conventional channels for information of similar classification. It is essential, however, that reference to the existence or nature of COMINT or any COMINT activity, either direct or indirect, be avoided except among those to whom the knowledge is necessary for the proper performance of their duties.

3. Information related to COMINT or COMINT activities which indicates a degree of success or progress in the production of COMINT, a sophisticated COMINT technique or the scale and direction of COMINT effort to a degree which may stimulate countermeasures, as specified in Annex A hereto, must be safeguarded precisely as though it were COMINT. Except as provided hereinafter, documents containing such information, including messages transmitted electrically, shall be transmitted only via COMINT channels, and shall bear the classification and COMINT codeword appropriate to the most sensitive category or sub-category of COMINT to which they relate.

4. Information related to COMINT or COMINT activities, specified in Annex B hereto, shall be kept exclusively within COMINT channels, except as provided for hereinafter and in that Annex. Documents which contain such information,

- 1 -

5115

Approved for Release by NSA on 04-04-2013, FOIA Case #100386 (Litigation)

~~TOP SECRET DAUNT~~

NSA IS CONTROL NO 02143
COPY NUMBER
PAGES

NSA FOIA Case 100386 Page 00032

Doc ID: 6613059

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

including messages transmitted electrically, shall bear the appropriate classification but no COMINT codeword, and shall be clearly identified by the caveat "HANDLE VIA COMINT CHANNELS ONLY", stamped, typewritten, or printed on each page. In the case of bound documents, the identification will show on the cover and title page, if any.

5. Information pertaining to COMINT or COMINT activities, specified in Annex C hereto, may be handled in accordance with normal practice for other information of similar classification. However, nothing herein should be construed as prohibiting an authority from passing such information in COMINT channels. (In such cases, the caveat "HANDLE VIA COMINT CHANNELS ONLY" will not be used.)

SPECIAL USAGE

6. Should it become necessary to furnish information of the types listed in Annex A to non-indoctrinated persons, such action will be taken only after specific authorization in each case by proper authority designated by USIB or LSIB. When a document containing such information is released from COMINT channels, the codeword must be removed. NSA and GCHQ, through technical channels, will undertake to keep the other party informed, at least in general terms, of the material involved.

7. Information related to COMINT or COMINT activities of the types listed in Annex B may be furnished to non-indoctrinated persons, only with the prior approval of the originator or proper authority and in accordance with the procedures established by USIB or LSIB. When a document containing such information is released from COMINT channels, the handling caveat must be removed or rendered illegible.

8. Every reasonable precaution must be taken to ensure that documents released from COMINT channels are given minimum distribution and receive the security protection their contents warrant.

9. Working papers and similar documents containing information of the types listed in Annexes A and B need not, at the discretion of the officer in charge and after full consideration of the risks involved, bear the classification, codeword or handling caveat when handled exclusively within a COMINT secure area by indoctrinated persons.

~~TOP SECRET DAUNT~~

59 02143
PAGES

NSA FOIA Case 100386 Page 00033

Doc ID: 6613059

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

CLASSIFICATION

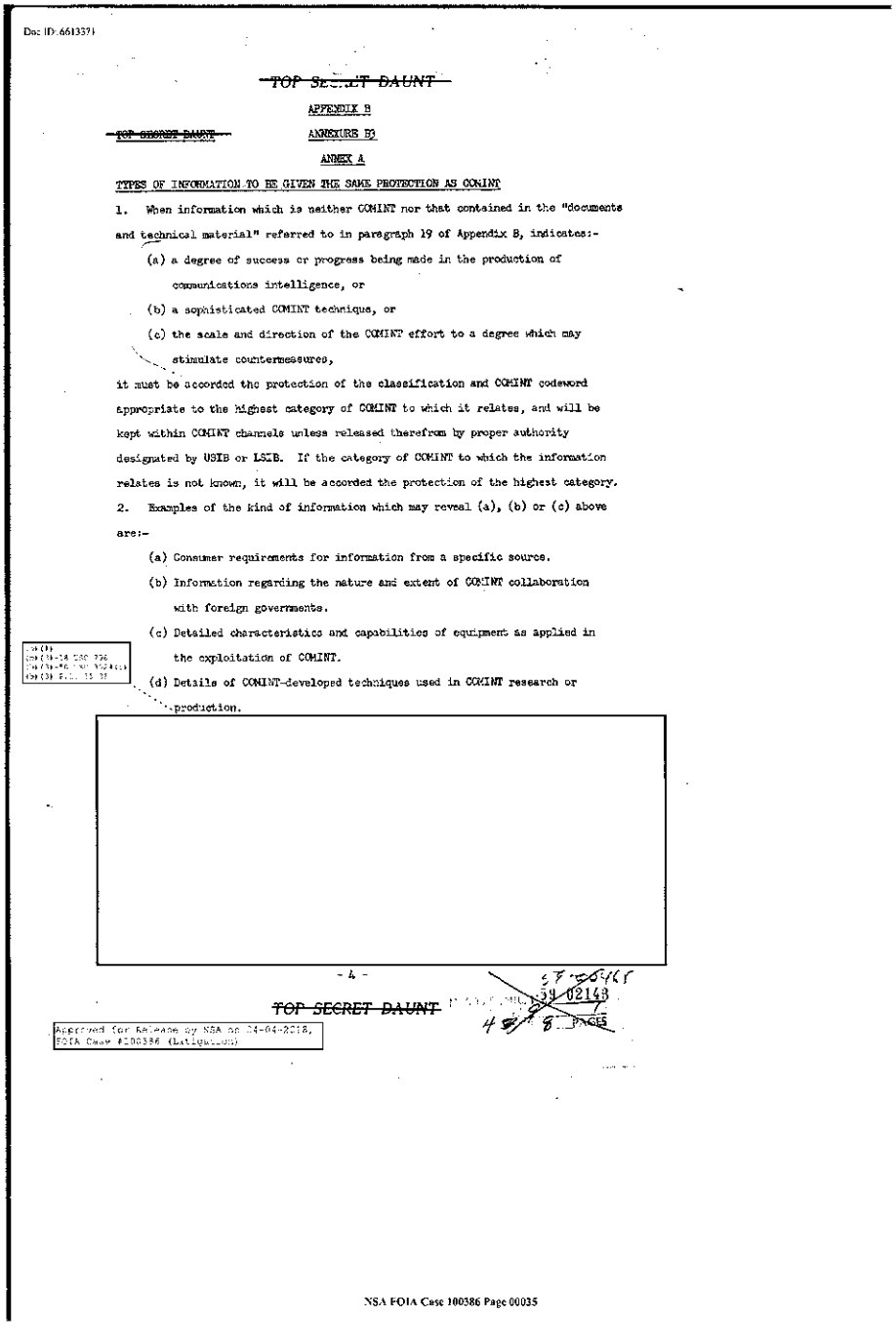
10. The classification of each document containing information related to COMINT or COMINT activities must be determined individually, after due consideration of the damage which unauthorized disclosure of its contents could cause to national security, national interests, and the capability of either party to continue to produce communications intelligence.

PUBLIC STATEMENTS

11. Maximum feasible administrative action will be taken to require that all public statements which may contain information related to COMINT or COMINT activities are submitted, for preliminary review and advice, to the appropriate COMINT authority, as specified by either Board. In the event that such information already publicly revealed is included in a document submitted by a private source for review, an attempt by persuasion shall be made to eliminate such information or to express it in such general terms as to conceal, to the maximum degree possible, specific associations with COMINT activities. In the event such a document is submitted by an official source, that document will be classified in accordance with paragraph 10 above.

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00034



Doc ID: 6613371

~~TOP SECRET DAUNT~~

APPENDIX B

~~TOP SECRET DAUNT~~ ANNEXURE B3

ANNEX A

TYPES OF INFORMATION TO BE GIVEN THE SAME PROTECTION AS COMINT

1. When information which is neither COMINT nor that contained in the "documents and technical material" referred to in paragraph 19 of Appendix B, indicates:-

(a) a degree of success or progress being made in the production of communications intelligence, or

(b) a sophisticated COMINT technique, or

(c) the scale and direction of the COMINT effort to a degree which may stimulate countermeasures,

it must be accorded the protection of the classification and COMINT codeword appropriate to the highest category of COMINT to which it relates, and will be kept within COMINT channels unless released therefrom by proper authority designated by USIB or LSIB. If the category of COMINT to which the information relates is not known, it will be accorded the protection of the highest category.

2. Examples of the kind of information which may reveal (a), (b) or (c) above are:-

(a) Consumer requirements for information from a specific source.

(b) Information regarding the nature and extent of COMINT collaboration with foreign governments.

(c) Detailed characteristics and capabilities of equipment as applied in the exploitation of COMINT.

(d) Details of COMINT-developed techniques used in COMINT research or production.

[redacted]

- 4 -

~~TOP SECRET DAUNT~~

Approved for Release by NSA on 04-04-2018, FOIA Case #100386 (Litigation)

NSA FOIA Case 100386 Page 00035

Doc ID: 6613372

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~ APPENDIX B

ANNEXURE B

ANNEX B

TYPES OF INFORMATION TO BE HANDLED VIA COMINT CHANNELS ONLY

1. Information which does not require codeword protection but which relates to COMINT or COMINT activities will bear the classification indicated (but no codeword), will carry the caveat "HANDLE VIA COMINT CHANNELS ONLY" and be retained in COMINT channels unless exempted or released in accordance with procedures established by USIB or LSIB.

TOP SECRET

2. Information relating to COMINT or COMINT activities will be classified TOP SECRET if the unauthorized disclosure of it could result in exceptionally grave damage to national security, national interests or the continued conduct of COMINT operations. Examples of the kind of information which may warrant this classification are:-

(a) A plan, doctrine or policy or information on tasking or control which reveals specific COMINT operations of major importance.

(b) Information revealing the extent or nature of COMINT collaboration with specific foreign governments, including written agreements establishing such collaboration.

(c) Details of COMINT arrangements with Third Parties.

(d) Construction and budgetary information of major importance relating to COMINT collection and processing organizations and installations.

(e) Safe combinations permitting access to COMINT or information regarding COMINT activities.

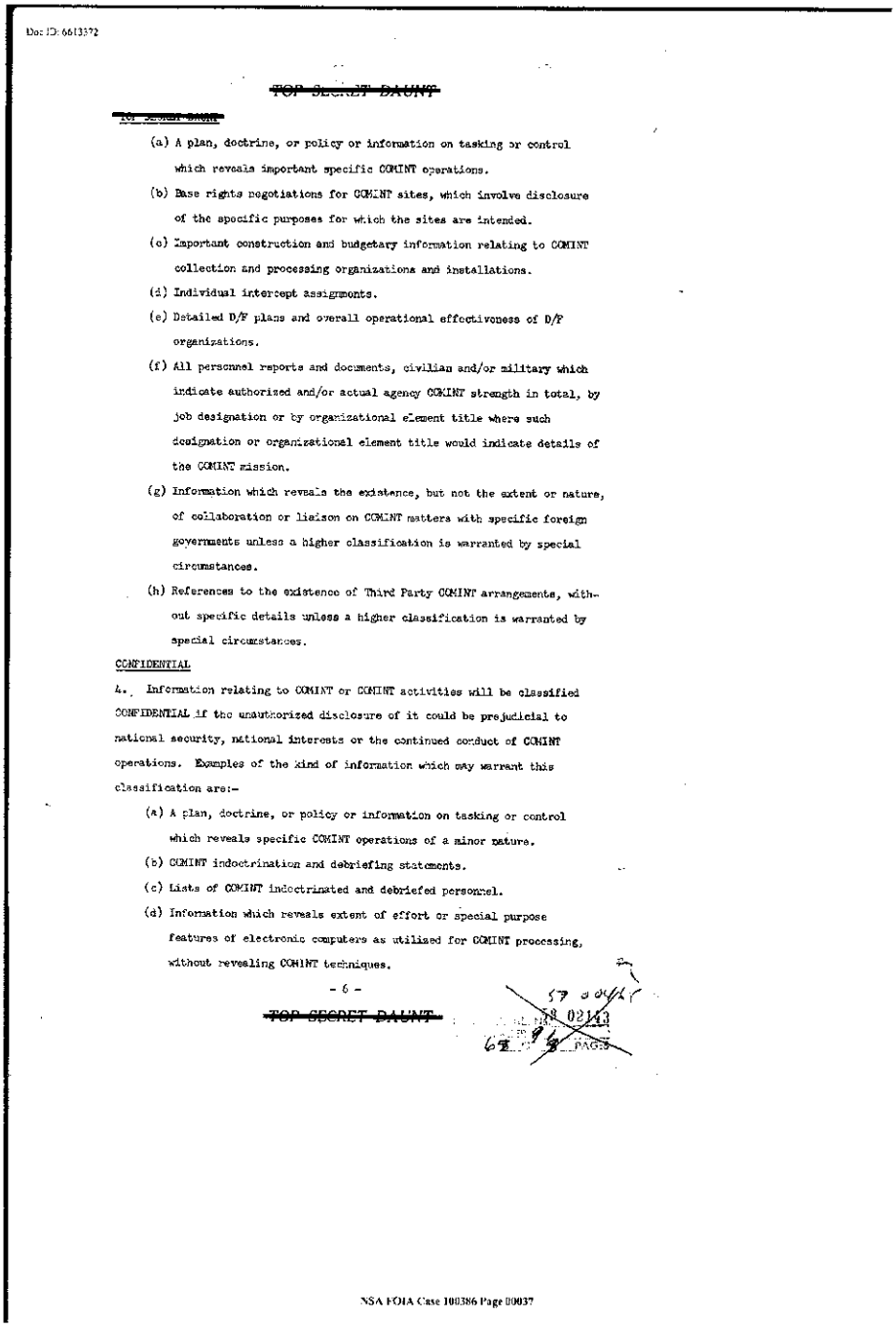
SECRET

3. Information relating to COMINT or COMINT activities will be classified SECRET if the unauthorized disclosure of it could result in serious damage to national security, national interests or the continued conduct of COMINT operations. Examples of the kind of information which may warrant this classification are:-

~~TOP SECRET DAUNT~~

Approved for Release by NSA on 04-04-2014, FOIA Case #100386 (litigation)

NSA FOIA Case 100386 Page 00036



Doc ID: 6613372

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

(a) A plan, doctrine, or policy or information on tasking or control which reveals important specific COMINT operations.

(b) Base rights negotiations for COMINT sites, which involve disclosure of the specific purposes for which the sites are intended.

(c) Important construction and budgetary information relating to COMINT collection and processing organizations and installations.

(d) Individual intercept assignments.

(e) Detailed D/F plans and overall operational effectiveness of D/F organizations.

(f) All personnel reports and documents, civilian and/or military which indicate authorized and/or actual agency COMINT strength in total, by job designation or by organizational element title where such designation or organizational element title would indicate details of the COMINT mission.

(g) Information which reveals the existence, but not the extent or nature, of collaboration or liaison on COMINT matters with specific foreign governments unless a higher classification is warranted by special circumstances.

(h) References to the existence of Third Party COMINT arrangements, without specific details unless a higher classification is warranted by special circumstances.

CONFIDENTIAL

4. Information relating to COMINT or COMINT activities will be classified CONFIDENTIAL if the unauthorized disclosure of it could be prejudicial to national security, national interests or the continued conduct of COMINT operations. Examples of the kind of information which may warrant this classification are:-

(a) A plan, doctrine, or policy or information on tasking or control which reveals specific COMINT operations of a minor nature.

(b) COMINT indoctrination and debriefing statements.

(c) Lists of COMINT indoctrinated and debriefed personnel.

(d) Information which reveals extent of effort or special purpose features of electronic computers as utilized for COMINT processing, without revealing COMINT techniques.

- 6 -

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00037

Doc ID 6613061

~~TOP SECRET DAUNT~~

~~TOP SECRET DAUNT~~

APPENDIX B

ANNEXURE B3

ANNEX C

TYPES OF INFORMATION WHICH MAY BE HANDLED IN ACCORDANCE WITH NORMAL SECURITY REGULATIONS

1. Information pertaining to COMINT which neither requires codeword protection nor the caveat "HANDLE VIA COMINT CHANNELS ONLY" will be classified and handled in accordance with U.S. or U.K. governmental security regulations in effect for information unconnected with COMINT or COMINT activities.

SECRET

2. Information, the unauthorized disclosure of which could result in serious damage to national security or national interests, will be classified SECRET. Examples of the kind of information which may warrant this classification are:-

(a) Construction and budgetary matters pertaining to COMINT collection or processing organizations and installations, provided no reference is made to their specific functions.

(b) Base rights negotiations for COMINT sites, provided no mention is made of actual purposes for which the sites are intended.

CONFIDENTIAL

3. Information, the unauthorized disclosure of which could be prejudicial to national security or national interests, will be classified CONFIDENTIAL. Examples of the kind of information which may warrant this classification are:-

(a) Personnel reports and documents, civilian or military, which indicate authorized or actual COMINT agency strength in total, by organizational element, short title or symbol, by primary element, or by function.

(b) Regulations stating the general mission and functions of COMINT activities that do not reveal specific COMINT techniques or procedures.

(c) Correspondence on hazardous duty restrictions pertaining to individuals released from COMINT assignments.

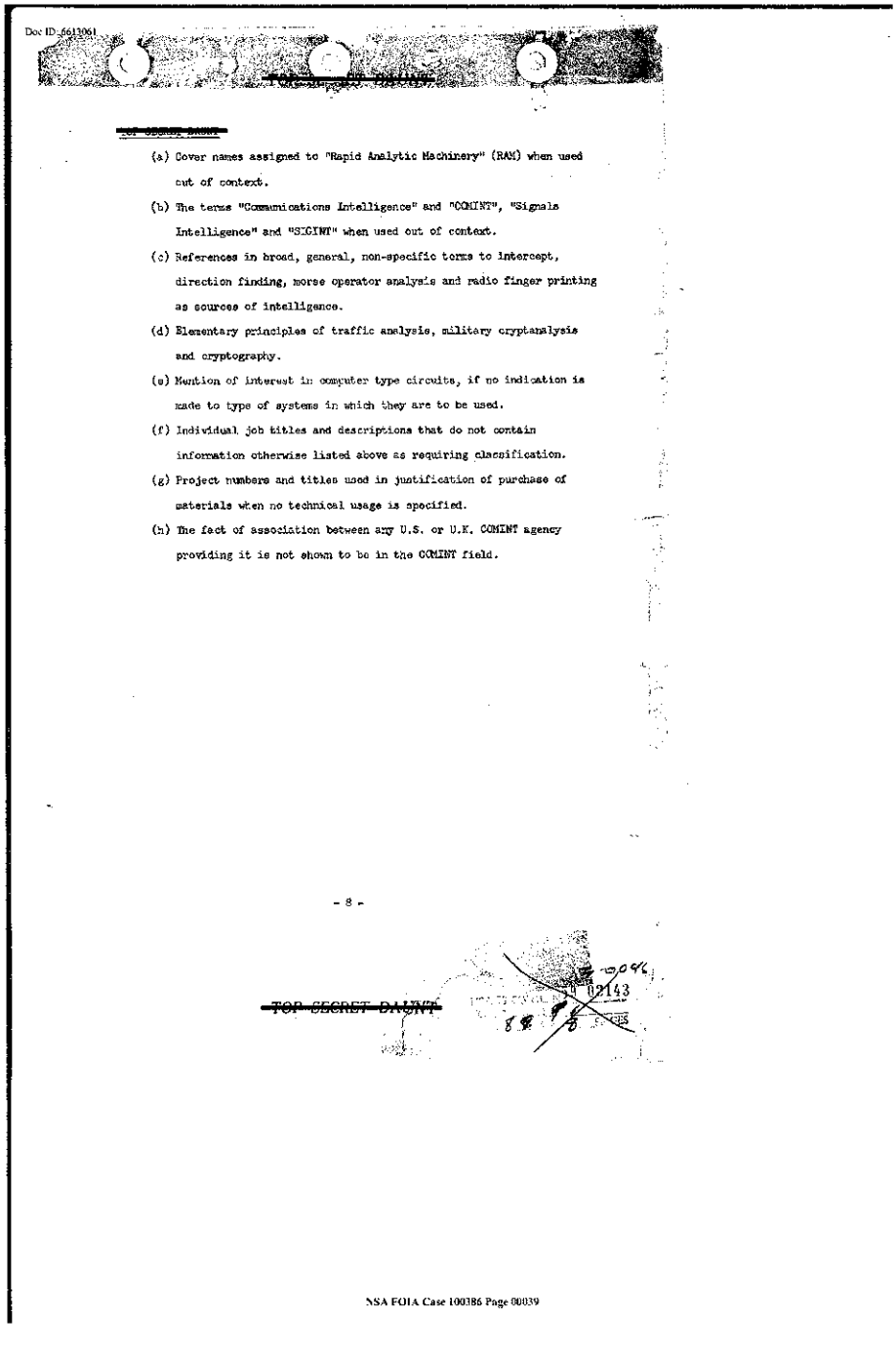
UNCLASSIFIED

4. Examples of the kind of information which is UNCLASSIFIED are as follows:-

Approved for Release by NSA on 04-04-2018, FOIA Case #100386 (Litigation)

~~TOP SECRET DAUNT~~

NSA FOIA Case 100386 Page 00038



Doc ID 6613061

~~TOP SECRET DAIVT~~

(a) Cover names assigned to "Rapid Analytic Machinery" (RAM) when used out of context.

(b) The terms "Communications Intelligence" and "COMINT", "Signals Intelligence" and "SIGINT" when used out of context.

(c) References in broad, general, non-specific terms to intercept, direction finding, morse operator analysis and radio finger printing as sources of intelligence.

(d) Elementary principles of traffic analysis, military cryptanalysis and cryptography.

(e) Mention of interest in computer type circuits, if no indication is made to type of systems in which they are to be used.

(f) Individual job titles and descriptions that do not contain information otherwise listed above as requiring classification.

(g) Project numbers and titles used in justification of purchase of materials when no technical usage is specified.

(h) The fact of association between any U.S. or U.K. COMINT agency providing it is not shown to be in the COMINT field.

- 8 -

~~TOP SECRET DAIVT~~

02143

NSA FOIA Case 100386 Page 00039

UNCLASSIFIED

UNCLASSIFIED
PAGE 01 CANBERR 03113 0106292
ACTION EAP-00
INFO LOG-00 COPY-01 ADS-00 INR-10 EUR-00 SS-00 CIAE-00
H-01 NSC-01 NSAE-00 HA-08 L-03 PM-10 PA-02
OMB-01 ACDA-12 USIE-00 SP-02 SNP-01 PRS-01 SPD-02
/055 W
----------127222 0106402 /21

R 0126002 APR 85
FM AMEMBASSY CANBERRA
TO SECSTATE WASHDC 1239
INFO SECDEF WASHDC
AMEMBASSY WELLINGTON
AMEMBASSY ATHENS
USIA WASHDC 5865
AMCONSUL SYDNEY
AMCONSUL MELBOURNE
AMCONSUL BRISBANE
AMCONSUL PERTH
UNCLAS CANBERRA 03113
E.O. 12356: N/A
TAGS: PARM, MARR, AS, US
SUBJECT: DEFMIN BEAZLEY DEFENDS PINE GAP
REF: CANBERRA 3075 (NOTAL)

1. ON MARCH 31, DEFENSE MINISTER KIM BEAZLEY WAS INTERVIEWED ON THE "SUNDAY" TELEVISION PROGRAM. HE WAS ASKED A NUMBER OF QUESTIONS RELATING TO REPORTS (REFTEL) THAT PINE GAP WAS BEING USED TO COLLECT INTELLIGENCE AGAINST GREECE AND MIGHT BE ALSO USED TO INTERCEPT AUSTRALIA'S OWN COMMUNICATIONS.
2. BEAZLEY STATED THAT HE WOULD CONTINUE TO ADHERE TO THE GOA POLICY OF NOT COMMENTING ON
UNCLASSIFIED
UNCLASSIFIED
PAGE 02 CANBERR 03113 0106292
SPECIFIC ALLEGATIONS ABOUT THE DETAILED OPERATIONS OF THE JOINT FACILITIES. HE SAID, HOWEVER, THAT IT WOULD BE A MISTAKE TO ASSUME THAT A REPLY OF "NO COMMENT" IMPLICITLY CONFIRMED WHATEVER ALLEGATIONS ABOUT THE JOINT FACILITIES WERE BEING MADE.

3. BEAZLEY ALSO STATED THAT THE GOA IS FULLY AWARE OF EVERYTHING THAT TAKES PLACE AT THE JOINT FACILITIES AND THAT GOA APPROVAL IS REQUIRED FOR ANY SPECIFIC ACTIVITY. BEAZLEY SAID THAT

IN DECIDING WHETHER OR NOT TO GIVE AGREEMENT FOR A PARTICULAR ASPECT OF THE JOINT FACILITIES, THE GOA MADE ITS DECISION "BASED ON THE FULLEST
UNCLASSIFIED / PAGE 1

YOUNG THOMAS S 04/01/85 095625 PRINTER: FD
85 CANBERRA 3113
UNCLASSIFIED
UNDERPINNING OF AUSTRALIAN FOREIGN POLICY AND OUR
OWN OBJECTIVES." BEAZLEY SAID THAT HE HAD MADE
THIS POINT TO ALP BACKBENCHERS WHO HAD ASKED
ABOUT THE FUNCTIONING OF THE JOINT FACILITIES.

4. BEAZLEY EXPLICITLY REJECTED THE SUGGESTION
THAT THE U.S. IS USING THE FACILITIES TO SPY ON
AUSTRALIA. HE AFFIRMED THAT THE GOA KNOWS
EVERYTHING THAT TAKES PLACE AT THE FACILITIES.
HE SAID THAT HE COULD MAKE THIS ASSURANCE BASED
ON AUSTRALIA'S OWN MONITORING, NOT SIMPLY ON
AMERICAN ASSURANCES. HE SAID "NOTHING HAPPENS AT
THESE FACILITIES ABOUT WHICH THE GOVERNMENT IS
UNAWARE. NOTHING CAN BE DONE AT THESE FACILITIES
WITHOUT THE ACQUIESENCE OF THE AUSTRALIAN
GOVERNMENT."

5. THE "AUSTRALIAN" NEWSPAPER APRIL 1 PRINTED
BEAZLEY'S REMARKS, PLUS AN ASSERTION BY ANU
UNCLASSIFIED
UNCLASSIFIED
PAGE 03 CANBER 03113 0106292
DEFENSE EXPERT DES BALL THAT BEAZLEY'S ASSURANCE
IS "SILLY." BALL CLAIMED THAT HE WAS SPOKEN TO
INDIVIDUALS WORKING AT PINE GAP AND THAT THERE
WERE AT LEAST TWO AREAS OF THE FACILITY WHERE
AUSTRALIAN NATIONALS ARE NOT PERMITTED ENTRY --
THE U.S. "NATIONAL COMMUNICATION AND CYPHER ROOM" — CORRECT, but Hayden when Shadow PM, did enter area once.
AND THE "KEY ROOM WHERE THEY (AMERICANS) DO THE
FINAL ANALYSIS OF ALL INCOMING INTELLIGENCE." — NO SUCH AREA -
BALL CHARGED THAT THIS SITUATION IS UNSATISFACTORY
AND THAT AUSTRALIAN NATIONALS SHOULD HAVE FULL
ACCESS TO ALL PARTS OF THE FACILITY.

6. THE "AUSTRALIAN" ALSO CARRIED A SEPARATE ARTICLE
BY ITS DEFENSE EXPERT PETER YOUNG WHO IS CURRENTLY
IN AUCKLAND. YOUNG CLAIMED THAT THE CONSENSUS
AMONG INTELLIGENCE EXPERTS IS THAT THERE IS NO
SUBSTANCE TO THE CHARGE THAT THE REPOSITIONING
OF A U.S. SATELLITE WAS DESIGNED TO SPY ON GREEK
COMMUNICATIONS. YOUNG SAID THAT "U.S. SOURCES
HAVE CONFIRMED THE SATELLITE HAS BEEN MOVED TO
ALLOW COVERAGE OF A DIFFERENCE FOOTPRINT. THEY
HAVE SAID THIS WAS INTENDED TO ALLOW CONTINGENCY
COVERAGE FROM ALTERNATIVE U.S. AND ALLIED GROUND
STATIONS IN THE REGION IN THE EVENT OF THE CLOSING
OF THESE FACILITIES BY THE LEFT-LEANING GREEK
GOVERNMENT." RESEN
UNCLASSIFIED

PAGE 2

C06489872 NO CLASSIFICATION MARKED

SECRET WITH
SECRET/NOFORN ATTACHMENT

5071

THE WHITE HOUSE
WASHINGTON

RELEASE IN FULL

MEMORANDUM FOR THE SECRETARY OF DEFENSE
THE ACTING DIRECTOR OF CENTRAL INTELLIGENCE

SUBJECT: Instructions for Sharing Classified Defense and Intelligence Information with the United Kingdom and Australia (C)

I have reviewed and approve the attached instructions for sharing classified defense information and intelligence information with the United Kingdom and Australia. I direct that you begin implementing this guidance immediately and that you complete implementation by June 1, 2005. Although these instructions shall remain internal to the United States Government, you are authorized upon issuance of these instructions to initiate appropriate discussions with your United Kingdom and Australian counterparts regarding necessary implementation actions. (S)

No modifications or amendments should be made to the joint instructions without prior coordination with me through the National Security Advisor. (U)

Please provide me through the National Security Advisor with a report of your implementation actions by September 30, 2004. In addition, please provide the National Security Advisor a report concerning the positive impact of these instructions on sharing with the United Kingdom and Australia by October 1, 2004. (S)

Second Party - UK

Attachment
Draft Instructions

cc: The Secretary of State

SECRET WITH
SECRET/NOFORN ATTACHMENT
Reason: 1.5(e)
Declassify on: 7/15/14

NO CLASSIFICATION MARKED

C06489887

NO CLASSIFICATION MARKED

THE WHITE HOUSE
WASHINGTON

July 19, 2004

RELEASE
IN FULL

The Right Honorable
Tony Blair, M.P.
Prime Minister
London

Dear Prime Minister:

We both agree that the close relationship between our governments requires the utmost cooperation in all areas. To further this cooperation, I have approved changes that will enhance the sharing of information between our defense and intelligence communities.

I have directed Secretary of Defense Rumsfeld and Acting Director of Central Intelligence McLaughlin to implement these changes immediately, and to coordinate with their respective British counterparts to ensure that the changes are making a difference in the field. My primary objective is to ensure the broadest possible sharing of relevant defense and intelligence information in the areas of planning and executing military and counterterrorism operations. Toward that end, Secretary Rumsfeld and Acting Director McLaughlin will be providing a status report to me by September 30, 2004, about their progress toward achieving this goal.

I am confident this effort will be of mutual benefit to the United States and the United Kingdom as we confront the very serious national security challenges facing our countries today and in the future.

As always, I appreciate your insights and the many contributions that the United Kingdom is making in our joint endeavors.

Sincerely,

George W. Bush

NO CLASSIFICATION MARKED

C06489888

NO CLASSIFICATION MARKED

THE WHITE HOUSE
WASHINGTON

July 19, 2004

RELEASE IN FULL

The Honorable
John Howard
Prime Minister of Australia
Canberra

Dear Prime Minister:

We both agree that the close relationship b[illegible]veen our governments requires the utmost cooperation in all areas. To further this c[illegible]ration, I have approved changes that will enhance the sharing of information between our d[illegible]se and intelligence communities.

I have directed Secretary of Defense Rumsfeld and Acting Director of Central Intelligence McLaughlin to implement these changes immediately, and to coordinate with their respective Australian counterparts to ensure that the changes are making a difference in the field. My primary objective is to ensure the broadest possible sharing of relevant defense and intelligence information in the areas of planning and executing military and counterterrorism operations. Toward that end, Secretary Rumsfeld and Acting Director McLaughlin will be providing a status report to me by September 30, 2004, about their progress toward achieving this goal.

I am confident this effort will be of mutual benefit to the United States and Australia as we confront the very serious national security challenges facing our countries today and in the future.

As always, I appreciate your insights and the many contributions that Australia is making in our joint endeavors.

Sincerely,

George W. Bush

NO CLASSIFICATION MARKED

C06519306

~~SECRET~~ UNCLASSIFIED

S/ES 200913997
xr 200913568

RELEASE IN FULL

THE SECRETARY OF STATE
WASHINGTON

July 28, 2009

Orig to WH
Dist to:
S
D(S)
D(L)
P
E
T
M
G
R
C
F
S/P
PA
S/ES
TMS
INR
EAP
ad

~~SECRET//NOFORN~~
DECL: MR

MEMORANDUM FOR NATIONAL SECURITY ADVISOR JONES

FROM: Hillary Rodham Clinton

SUBJECT: Paper PC on Lifting New Zealand Intelligence Sharing Restrictions

The Department of State concurs in the proposal to lift the remaining restrictions on intelligence sharing with the Government of New Zealand.

Department of State, A/GIS/IPS/SRP
Change to Unclassified
(X) Release ( ) Excise ( ) Deny ( ) Declassify
Exemptions b ( ) ( ) E.O. 13526 25x ( )( )( )
Declassify after _____
With concurrence of:
_____ obtained _____ not obt.
IPS by C. Rodriguez Date 3/14/2018

UNCLASSIFIED

~~SECRET//NOFORN~~
Classified by Hillary Rodham Clinton
E.O. 12958, Reasons: 1.6 (b) and (c)

~~SECRET~~

PRIVACY INTERNATIONAL

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471