LAWFARE

FIVE EYES

Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance

By **Scarlet Kim**, **Paulina Perlin** Monday, March 25, 2019, 9:11 AM

In July 2017, Privacy International and Yale Law School's Media Freedom & Information Access Clinic (MFIA) filed a lawsuit against the National Security Agency, the Office of the Director of National Intelligence (ODNI), the State Department, and the National Archives and Records Administration seeking access to records related to the Five Eyes alliance under the Freedom of Information Act. The Five Eyes alliance emerged from spying arrangements forged during World War II and facilitates the sharing of signals intelligence (SIGINT) among the U.S., the U.K., Australia, Canada and New Zealand.

At the time Privacy International and MFIA filed the lawsuit, the most recent publicly available version of the agreement governing the Five Eyes alliance—known as the UKUSA Agreement—dated back to 1955. That version of the agreement provides that the Five Eyes are to share, by default, all SIGINT they gather, as well as methods and techniques relating to SIGINT operations. An appendix to that agreement elaborates further that the Five Eyes are to share "continuously, currently and without request" both "raw" (that is, unanalyzed) intelligence in addition to "end product" (intelligence that has been subjected to analysis or interpretation).

Beginning in December 2017, the NSA and the State Department began making disclosures in response to the lawsuit. We've written previously about some of the records disclosed by the government and what they reveal about the government's approach to classification and publication of these types of agreements. In September 2018, the NSA released several additional batches of records, containing disclosures that significantly enhance our understanding of the history and nature of the UKUSA Agreement. Below, we summarize the most interesting of these disclosures and how they update what we know about the Five Eyes intelligence-sharing arrangement. Privacy International has also made available on its website the records the government disclosed. Nevertheless, critical questions regarding the Five Eyes alliance, including its implications for the constitutional rights of Americans, remain.

Snapshots of the UKUSA Agreement from the 1970s to the 1990s

Among the records the government has produced is a series of documents, dating from the 1970s to the 1990s, that aid our understanding of the history and nature of the UKUSA Agreement, particularly as it has evolved over time.

"Historical Note on the UKUSA COMINT Agreement" (Oct. 27, 1972) (attaching President Truman Memorandum [Sept. 12, 1945])

In 1972, a historical officer at the NSA produced a "Memorandum for the Record" entitled

"Historical Note on the UKUSA COMINT Agreement," which provides further insight into the formation of the agreement. It begins by noting that "[t]he question occasionally arises as to the governmental levels at which the UKUSA COMINT Agreement was authorized or approved" but quickly clarifies that "the President of the United States authorized an agreement in this field, and that the British Foreign Minister must have been aware of it." (Compare that with, for example, the statement by David Lange, the former prime minister of New Zealand, who remarked that "it was not until I read [the] book ["Secret Power" by Nicky Hager, which details the history of New Zealand's Government Communications Security Bureau] that I had any idea that we had been committed to an international integrated electronic network." He continued that "it is an outrage that I and other ministers were told so little, and this raises the question of to whom those concerned saw themselves ultimately answerable.")

As support for the NSA's history of the agreement, the memorandum attaches a 1945 memorandum from President Truman authorizing the then-secretary of war and the secretary of the Navy "to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States." This presidential memorandum is of particular interest because it provides evidence that the president directly authorized the various military branches to determine the future course and contours of the UKUSA Agreement. This arrangement has not necessarily been clear to the public (nor was it clear, based on the wording of the 1972 memorandum, to the NSA itself). Interestingly, President Truman's memorandum was not among the documents the NSA released in 2010 relating to the history of the UKUSA Agreement, which cover the period between 1940 and 1956.

"Description of SIGINT Relations between NSA and GCHQ" (December 1985)

In December 1985, the NSA produced what it described as "a review of the NSA-GCHQ [U.K. Government Communications Headquarters] SIGINT relationship including an assessment of the present value of the exchange and identifiable problems." The purpose of the review was "to serve as a basis for determining … plans for the conduct of this relationship in the future, for any improvements/changes regarding control and accountability of the existing exchange, as well as developing proposals for additional contributions which should be made by each party." The document provides one of the clearest explanations of the status of the UKUSA Agreement and a detailed overview of its scope and operation at this point in time.

With respect to the origins of the agreement, the "Background" section of the document describes how "SIGINT collaboration with the UK began in 1941 and was formalized in the UKUSA Agreement of 1946." Significantly, however, the section goes on to explain that the agreement "was so generally written that, with the exception of a few proper nouns, no changes to it have been made" and that "[t]he principles remain intact, allowing for a full and interdependent partnership." (The NSA's 2010 release of documents relating to the history of the UKUSA Agreement include both the original agreement and an updated version of the agreement, concluded in 1955, the main texts of which are nearly identical.)

The "Background" section notes that "[o]ver the years numerous appendices have been added [to the agreement] to cover specific areas of widening interest and ever-increasing sophistication." Annex B to the document—"A Description of the Appendices to the UKUSA Agreement"— is perhaps the most complete inventory that we have to date of the agreement's appendices and includes a short explanation of each appendix. Notably, Annex B divides the appendices into two categories —those "that may be amended only by board agreement" and those "which the directors, NSA and GCHQ, may change or interpret by mutual agreement."

The "Background" section further indicates that "Divisions of Effort (DOE) and/or understandings between NSA and GCHQ are undertaken to respond to existing requirements." (Annex C to the document—"Details of UKUSA Division of Effort"— may offer further details on how DOEs are concluded and what they cover but is entirely redacted.) Later in the document, in a section called "Areas of Cooperation/Exchange," the NSA admits that while "[t]here are many MOA's [Memoranda of Agreement] and MOU's [Memoranda of Understanding] between the parties; however, a significant amount of division of effort is accomplished without any formal DOE or MOU and has evolved through cooperation engendered by personal contact and exchange." The document then notes that "[a]n understanding is created on each target of mutual interest in terms of collection, processing and reporting."

The document offers some insight into how the two agencies manage this kind of fluid and informal division of effort. In addition to integrating analysts into each other's headquarters and running joint operations, the two agencies exchange "[a] great number of visits" from "various levels of personnel from the Directorate down" ranging from "analyst-to-analyst discussions, conferences, periodic meetings, management/planning reviews and consultations, [and] Directorate level policy decisions." In addition, the two agencies hold a number of conferences, typically "on an annual basis" with two of the most significant being the "Program Management & Review" and "Joint Management Review" conferences. The former involves "Senior Management participation" while the latter involves "Senior Management, at Deputy Director level,

participation." (Additional conferences listed are redacted.) (Privacy International has previously discussed the extent and nature of Five Eyes coordination in a report and in its ongoing case against the U.K. government, which challenges, among other issues, its access to intelligence gathered by the U.S. government.)

In addition to clarifying the nature of the original UKUSA Agreement and how the NSA and the GCHQ have adapted it over time, this document confirms our understanding of the broad scope of the UKUSA Agreement. In the "Background" section, it observes that "the basic agreement … for the exchange of all COMINT results including end product and pertinent collateral data … for targets worldwide, unless specifically excluded from the agreement at the request of either party" has "[o]ver the years … been the case." In its high-level "Findings/Conclusions," it also documents that "[t]here is a heavy flow of raw intercept, technical analytic results, and SIGINT product between NSA and GCHQ." Additional language contained in the "Findings/Conclusions" section has been redacted. And in its concluding "Areas of Cooperation/Exchange" section, it indicates that "GCHQ-NSA SIGINT exchange involves a sharing of a wide variety of targets worldwide, ranging from military activities to [REDACTED] terrorist activities, and [REDACTED]" and "includes the exchange of material (raw intercept, analytic, product) on [REDACTED]." The document hints at how the two agencies facilitate such sharing in practice, including by ensuring that the "GCHQ has direct access to NSA computer systems."

Finally, the "Background" section notes that the nature and scope of the agreement between the NSA and the GCHQ extends to third-party countries as well. It explains that "the agreement makes provision for obtaining agreement between the two partners for COMINT relationships established with Third Parties and to ensure that materials received from such Third Party arrangements are made available to GCHQ and NSA." It adds that "special consideration" has been given to "Canada, Australia, New Zealand and to not consider them as Third Parties." (This special consideration is documented in Appendix J of the 1955 version of the agreement and gives rise to what we now know as the Five Eyes Alliance.)

"Review of US-UK Exchange Agreement" (Jan. 25, 1994) (attaching "Review of US-UK Exchange Agreement" [Nov. 18, 1993])

In 1994, the NSA director of foreign relations issued an action memorandum, which appears to request input from various divisions within the agency regarding another review of the UKUSA Agreement. The memorandum notes that the purpose of the review is to "satisfy the foreign reviews and audits currently underway with Congressional, DoD [Department of Defense], and GAO [Government Accountability Office] staffs, in addition to providing a comprehensive study of current exchange policies with GCHQ." The memorandum further notes that the Operations Directorate had already initiated "an operational review … to include a list of what is not currently exchanged with the British, what we should not exchange in the future, and new things that should be exchanged in the future," documented in a 1993 memorandum included as Attachment A. The 1994 memorandum also indicates that a second attachment consists of a template for presenting "(1) by country, and (2) by topic … exactly what is exchanged in terms of raw traffic, product and technical reports, [REDACTED] technology, etcetera." Finally, it orders that "[w]here possible," "copies of any Memorandums of Understanding or Divisions of Effort between NSA and GCHQ be provided in support of the exchanges [REDACTED]."

The most interesting aspect of this disclosure is the attached 1993 memorandum, which describes the Operations Directorate's ongoing operational review of the UKUSA Agreement. First, it states that there is "no single document [that] exists in sufficient detail to serve as such an agreement," confirming to some extent the description of the evolution of the UKUSA Agreement in the 1985 document discussed above. Second, it admits that "to list what IS shared would be extremely expensive in terms of required man-hours." It therefore proposes "to break the task into three parts," consisting of (1) "[l]isting in sufficient detail those things that are not (to the best of your knowledge) exchanged with the UK today," (2) "those things that managers and senior technical experts believe may well need to be altered or declared unexchangeable in the near future (5-8 years out or less)," and (3) "those new things that should be exchanged with the UK in the future."

"U.S. Cryptologic Partnership with the United Kingdom" (May 1997)

In 1997, the NSA produced a background paper on the "US-UK Cryptologic relationship" for President Clinton in advance of his upcoming meeting with then-U.K. Prime Minister Tony Blair. The paper describes the relationship as "based on a formal 'UKUSA Agreement,' which was signed in 1946, and includes numerous supporting agreements signed over the years with NSA's counterpart, the Government Communications Headquarters (GCHQ)." The paper also confirms that the agreement's

original understanding of "unrestricted" exchange "except for those areas that are specifically excluded (e.g. U.S. ONLY information) at the request of either party" continues into this period. The language immediately following this statement is redacted.

One line stands out in particular: "Some GCHQ [REDACTED] exist solely to satisfy NSA tasking." The unredacted portion of this sentence may indicate that the NSA is—or, at least, was—directly outsourcing certain SIGINT activities to the GCHQ. What we know about the purpose of the UKUSA Agreement certainly suggests this type of activity could fall within its scope. Appendix C of the 1955 version of the UKUSA Agreement discusses how the object of the agreement "is to ensure that maximum advantage is obtained from the combined available personnel and facilities of both parties." Government officials have also acknowledged the pooling of resources among the Five Eyes. Former Defense Secretary Caspar Weinberger, for example, has observed that the "United States has neither the opportunity nor the resources to unilaterally collect all the intelligence information we require. We compensate with a variety of intelligence sharing arrangements with other nations in the world." But the language contained in the background paper is a particularly stark suggestion of outsourcing.

"An Assessment of the UKUSA Relationship: Where We Go From Here" (undated)

This undated document is authored by one of the NSA's special U.S. liaison officers (SUSLO-4). SUSLO-4 describes it as "an honest effort … to describe the strengths and weaknesses of the UKUSA relationship so that NSA might better be able to make some hard decisions about the future of the relationship." This document is a particularly fascinating disclosure because it is one of the few to reveal and discuss tensions in the UKUSA relationship. While much of the document is redacted, the language that has not been expresses alarm regarding certain aspects of the NSA-GCHQ relationship.

The document notes particular concern regarding the exchange of personnel between the two agencies. It indicates that "[a]side from the respective liaison staffs, NSA and GCHQ exchange large number of integrees" and that "in recent years, some operational and staff elements in GCHQ have begun to use integrees as their representatives, and some integrees have assumed liaison-like functions." The document continues, noting that "[m]aking matters worse has been a recent trend to send integrees to function as special assistants, sometimes to alpha plus-one components working sensitive missions" meaning that "they also serve as lobbyists for GCHQ seniors in policy matters."

Below, we discuss several newly released NSA policy documents, which clarify the policies governing Five Eyes partner access to U.S. SIGINT and help elucidate the distinction between a liaison and an integree. USSID FA6001, which addresses "Second Party SIGINT Relationships," describes the "Special United States Liaison Officer (SUSLO)" as "represent[ing] ODNI … in all SIGINT relationships with that Second Party, and, in so doing, execut[ing] National Intelligence Board (NIB) policy guidance." Presumably, liaison officers from the other Five Eyes partners play a similar role vis-a-vis the United States. By contrast, NSA/CSS [Central Security Service] Policy 1-13, which addresses the policies and procedures for integrating Five Eyes partner employees into the NSA defines "Second Party Integrees" as individuals "who … are working solely under the direction and operational control of the DIRNSA/CHSS [Director of the NSA/Chief of the Central Security Service] to conduct cryptologic or information assurance activities that support NSA/CSS mission." In other words, whereas the role of a liaison officer is to explicitly advocate for the interests and policies of the second party that they represent, the role of an integree is more operational in nature and intended to support the activities of the host agency.

The document provides two specific, troubling examples regarding integrees. First, it described how a GCHQ official "[r]ecently … lobbied hard to place an integree in" a particular position within the NSA, which the NSA "rightly rejected … as it would give GCHQ insight into certain sensitive operations we do not share." Second, it described how "[i]n another instance a strategically placed GCHQ drafted an MOA that committed [REDACTED] assistance from NSA to GCHQ" and concluded that "without addressing the correctness of this assistance, the propriety of this situation is disturbing." The second example is of particular interest because the disclosures as a whole reveal that the UKUSA Agreement's evolution over time has taken place through the exchange of MOUs/MOAs and DOEs (and, in some instances, without any written documentation). This example suggests a lack of oversight, at least at the time the document was written, as to how all these various arrangements are hashed out.

Indeed, the document then points to a broader lack of organization and control over the UKUSA relationship. It notes that whether it is exchanging SIGINT or integrees, the mode of interfacing with the GCHQ evolves based on myriad decisions at various levels within the NSA. It asks:

> Do we need to have an overall policy to ensure that these agreements are consistent with our plans for the future? For instance, should we determine a modus vivendi for exchange of integrees? Should the type of work be limited by charter? Should there be a common NSA position on the number and kind of electronic interfaces between NSA and GCHQ? Should the number be driven by NSA design or by GCHQ needs?

Five Eyes Partner Access to U.S. SIGINT

Among the records that the government has produced are several previously unreleased NSA policy documents, all dated within the past seven years, that illuminate a long-opaque feature of the Five Eyes relationship—the policies governing Five Eyes partner access to U.S. SIGINT.

USSID FA6001—"Second Party SIGINT Relationships" (Aug. 22, 2012)

U.S. Signals Intelligence Directive FA6001 addresses the many ways that U.S. SIGINT flows throughout the Five Eyes, albeit at a high level. Specifically, Annex B of the directive discusses the "Release of U.S. SIGINT Information to Second Party SIGINT Organizations" and notes that Five Eyes partners:

- Collaborate on a wide range of targets, with MOUs or DOEs, which are provided to the NSA/CSS Office of Corporate Policy, documenting the specific targets and degree of collaboration.
- "[R]eceive raw traffic, technical material, and serialised SIGINT reports derived from the U.S. effort on mutual targets."
- Receive "intelligence information on issues impacting international relations, and on events related to the partners' political, economic, military, or security interests."

Though this annex partially answers how the U.S. shares information with its Five Eyes partners, it also raises more questions: What is the scope of "targets" for which the countries collaborate? How "targeted" are they? And what kinds of authorization processes do each of the agencies undergo before agreeing to collaborate on mutual "targets"? Despite what we've learned at a general level about the content and nature of Five Eyes information sharing, these more specific contours remain largely unknown.

Signals Intelligence Directorate Management Directive 427—"Access to Classified U.S. Intelligence Information for Second Party Personnel" (Sept. 14, 2015)

Signals Intelligence Directorate Management Directive 427 is originally dated Aug. 1, 2009, but was subsequently revised on Dec. 28, 2013, and more recently on Sept. 14, 2015. This directive is most notable for its discussion of Five Eyes partner access to data that haven't been evaluated for foreign intelligence value or gone through the minimization process. The directive addresses Five Eyes personnel access to "NSA-CSS maintained databases or data sets" and then specifies that such databases or data sets should "only contain classified information marked releasable to that partner" or be "capable of restricting access only to that data which is marked as releasable to that partner."

The value of these limitations depends on the definitions of "databases" and "data sets." The directive later defines a data set as "a large collection of intelligence data that has not been evaluated for foreign intelligence or minimized to protect U.S. identities but is not a formal database subject to the SIGINT Contact Center (SCC) process" and may also be "[a] data feed such as would be needed for a research/development effort." This definition suggests that data sets may contain "data that has not been evaluated for foreign intelligence or minimized to protect U.S. identities," which raises questions as to how the U.S. restricts in practice what should or shouldn't be accessible to their Five Eyes partners.

The directive defines a database as "a structured collection of records or data that is stored in a computer system and organized in a data management system for quick retrieval of those records." It further notes that a database "is generally subject to the SCC process or a similar access control" but does not clarify what the SCC process is or to what (other) extent the data have been evaluated or minimized before being retained in a database.

The directive also discusses, although at a very high level, the procedures before a Five Eyes partner can access data. For partners working from within their own country's SIGINT agency, there appears to be a registration process in addition to training and auditing. However, the Snowden disclosures revealed how insubstantial training for NSA analysts can be, which continues to raise doubts about training requirements for Five Eyes partners. For Five Eyes partners who are integrated within a U.S. SIGINT component, there's a requirement to list databases or data sets that they've accessed.

NSA/CSS Policy 6-20—"Second Party Access to NSA/CSS TS/SCI Classified Information System" (Nov. 8, 2016)

NSA/CSS Policy 6-20 is originally dated March 31, 2014, but was revised Nov. 8, 2016. Though this policy mainly addresses the grainier details of Five Eyes partner access to NSA systems, it also holds some interesting insights.

The policy cites the UKUSA Agreement as its governing basis for information sharing (as do the two policy documents discussed above). However, this policy also notes the existence of "subsequent bilateral understandings with each Second Party partner," before proceeding to outline three relevant bilateral understandings, although two out of the three are redacted. The policy also notes, as a more general matter, that MOUs shall govern system connection and access policy and that these documents will be maintained by the Office of Policy.

The policy also mentions that Five Eyes partners are explicitly prohibited from accessing "U.S.-only keying materials or Nuclear Command and Control Information Assurance Materials (NCCIM)." However, the policy does not define "U.S.-only keying materials" and it is not clear what types of materials would fall under this category. It therefore says little about the bounds of what Five Eyes partners may and may not view.

NSA/CSS Policy 1-13—"Second Party Integrees" (Dec. 31, 2014)

NSA/CSS Policy 1-13 addresses the policies and procedures for integrating Five Eyes partner employees into the NSA. The NSA also disclosed what appears to be a forerunner of this document, a NSA/CSS Directive on "Second Party Integrees" dated Nov. 26, 1990. Both documents may be of interest in light of the discussion above of the undated record, "An Assessment of the UKUSA Relationship: Where We Go From Here," which raises concerns regarding GCHQ integrees and the lack of policy governing them.

Questions, Answers … and More Questions

Taken together, these documents begin to flesh out some of the unknowns surrounding the Five Eyes relationship. Thanks to this litigation, we've learned much more about the UKUSA Agreement's history and evolution, as well as its current policies governing the flow of U.S. SIGINT within the Five Eyes. However, while these documents have answered some of our questions, they continue to leave many others unaddressed and have prompted even more.

For example, these disclosures have helped clarify the basis of the Five Eyes alliance, which appears to continue to be the general language of the original 1946 agreement, supplemented by appendices and a potentially dizzying array of memoranda of understanding and divisions of effort (not to mention more informal arrangements). Yet the government was unable to locate, let alone produce, most of these additional records. That failure suggests continuing challenges to manage a sprawling intelligence-sharing enterprise, hinted at in the disclosures discussed above. Without clear sight of these various records forming the UKUSA Agreement, we continue to remain in the dark about the overall nature and scope of intelligence sharing among the Five Eyes, particularly as it is carried out today.

Even more troubling, we still don't know the rules, if they exist, that govern U.S. intelligence agencies' access to and dissemination of Americans' private communications and data. What happens to U.S. persons' information when it's collected by partner agencies? When it's collected by the U.S. and shared with partner agencies? Whether purposely or inadvertently? Does the U.S. allocate targeting efforts to partner agencies that may include the collection of U.S. persons' communications and data? If so, do the same rules apply as when the U.S. collects those persons' communications and data directly? The government has so far failed to produce any documents that address these questions. While we've further elucidated some of the history of the UKUSA Agreement and nature of the Five Eyes relationship, we still don't fully understand their impact on the constitutional rights of Americans.

Tags: NSA, National Security Agency, Freedom of Information Act (FOIA), Five Eyes

---

Scarlet Kim was formerly a Legal Officer at Privacy International, a UK-based human rights NGO focused on issues arising at the intersection of privacy and technology. Scarlet also previously worked as an Associate Legal Adviser at the International Criminal Court and as a Gruber Fellow in Global Justice at the New York Civil Liberties Union. She served as a clerk on the U.S. District Court for the Eastern District of New York and is a graduate of Yale Law School. She is a U.S.-qualified lawyer and is admitted as a Solicitor in England and Wales.

Paulina Perlin is a J.D. candidate at Yale Law School.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

PRIVACY INTERNATIONAL
62 BRITTON STREET
LONDON, EC1M 5UY, UNITED KINGDOM

Plaintiffs,

v.

NATIONAL SECURITY AGENCY,
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE,
DEPARTMENT OF STATE, and
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Defendants.

Civil Action No. _____

COMPLAINT

Plaintiff, Privacy International, by its undersigned attorneys, alleges:

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, *et seq.*, for declaratory, injunctive, and other appropriate relief brought by Privacy International, a non-profit, non-governmental organization that defends the right to privacy around the world and seeks to ensure that government surveillance complies with the rule of law.

2. By this action, Privacy International seeks to compel the National Security Agency ("NSA"), the Office of the Director of National Intelligence ("ODNI"), the Department of State ("State"), and the National Archives and Records Administration ("NARA") (collectively, "Defendants") to release requested records relating to the government's agreement to exchange signals intelligence with the governments of the United Kingdom ("U.K."), Canada, Australia and New Zealand (collectively, "Five Eyes alliance").

3. 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. Pursuant to 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.

4. A 1955 revision of the UKUSA Agreement is the most recent version of the agreement to be have been made public. Communications methods have dramatically changed since 1955. The development of new technology, especially 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. These advancements vastly increase the opportunities for governments to acquire, store and/or analyze communications and data and to share that information with other governments.

5. The nature of signals intelligence has also changed dramatically since 1955. As modern communications have evolved, intelligence agencies have developed more advanced ways to access, acquire, store, analyze and disseminate information.

6. How the government exchanges signals intelligence, and whether it appropriately accommodates the constitutional rights of American citizens and residents as well as the human rights of non-American citizens and residents, are matters of great public significance and concern.

7. Privacy International seeks access to the current text of the UKUSA Agreement, information about how the government implements the Agreement, and records concerning the standards and procedures for exchanging intelligence under the Agreement. These records are of

paramount concern because the public lacks even basic information about the Five Eyes alliance, including the current text of the Agreement and the rules and regulations that govern the government's access to and acquisition, storage, analysis and dissemination of Americans' communications as part of that arrangement. The public has equally scant information concerning the rules and regulations that govern the government's exchange of signals intelligence it has acquired, stored and/or analyzed with the other members of the Five Eyes alliance. This lack of transparency raises questions about whether the Five Eyes intelligence-sharing arrangement satisfies constitutional and statutory requirements.

8. Defendants have improperly withheld the requested records in violation of FOIA and in opposition to the public's strong interest in understanding the government's authority and legal basis for exchanging signals intelligence with other governments pursuant to the UKUSA Agreement.

PARTIES

9. Privacy International is a non-profit, non-governmental organization based in London, the U.K., that defends the right to privacy around the world. Privacy International is committed to ensuring that government surveillance complies with the rule of law and the international human rights framework. As part of this commitment, Privacy International seeks to ensure that the public is informed about the conduct of governments in matters that affect the right to privacy. Privacy International is a registered charity in the U.K. and its principal place of business is in London.

10. Defendant NSA is an intelligence agency established within the executive branch of the U.S. government and is an agency within the meaning of 5 U.S.C. § 552(f)(1).

11. Defendant ODNI is an intelligence agency established within the executive branch of the U.S. government and is an agency within the meaning of 5 U.S.C. § 552(f)(1).

12. Defendant State is a department of the executive branch of the U.S. government and is an agency within the meaning of 5 U.S.C. § 552(f)(1).

13. Defendant NARA is a department of the executive branch of the U.S. government and is an agency within the meaning of 5 U.S.C. § 552(f)(1).

JURISDICTION AND VENUE

14. This Court has subject-matter jurisdiction over this action and personal jurisdiction over Defendants pursuant to 5 U.S.C. § 552(a)(4)(B) and § 522(a)(6)(E)(iii). This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 5 U.S.C. §§ 701-06.

15. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B).

FACTS

History of the UKUSA Agreement

16. During World War II, the U.S. Army and Navy began independently developing signals intelligence relationships with their military counterparts in the U.K., Canada, Australia and New Zealand. In 1946, in the aftermath of the war, the London Signals Intelligence Board ("LSIB") (the predecessor to the Government Communications Headquarters ("GCHQ"), the U.K.'s present-day signals intelligence agency) and the State-Army-Navy Communication Intelligence Board ("STANCIB") (the body then coordinating U.S. signals intelligence activities) ratified the UKUSA Agreement to share signals intelligence.[1] *See* George F. Howe, *The Early*

[1] The original UKUSA Agreement was titled the "British-U.S. Communication Intelligence Agreement" and was later re-named the UKUSA Agreement.

History of NSA, Cryptologic Spectrum (1974), *available at* https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/early_history_nsa.pdf.

17. The NSA declassified the 1946 Agreement in 2010, along with 41 other documents relating to its formation, implementation, and alteration. All 42 documents are publicly available on the NSA's website. *See* UKUSA Agreement Release 1940-1956, NSA.gov (May 3, 2016), https://www.nsa.gov/news-features/declassified-documents/ukusa/.

18. As part of the 2010 series of declassifications, the NSA also declassified a 1955 revision of the UKUSA Agreement concluded between LSIB and the U.S. Communications Intelligence Board (which replaced STANCIB). *See* UKUSA Agreement ¶ 11 (Oct. 10, 1956), https://www.nsa.gov/news-features/declassified-documents/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"). A true and correct copy of the 1955 version of the UKUSA Agreement is annexed hereto as Exhibit A.

19. Upon information and belief, the 1955 UKUSA Agreement was a binding executive agreement, imbued with the force of law.

20. An appendix attached to the 1955 UKUSA Agreement reveals that Canada, Australia, and New Zealand officially joined the intelligence sharing alliance as "UK-USA collaborating Commonwealth Countries." *Id.* at ap. J ¶ 2.[2]

21. The 1955 UKUSA Agreement defines "communication intelligence" ("COMINT") as "all processes involved in, and intelligence information and technical material

[2] The appendices attached to the UKUSA Agreement are "considered integral parts" of the Agreement at the time of its amendment." UKUSA Agreement, *supra*, at "Introduction to the Appendices to the UKUSA Agreement."

resulting from, the interception and study of (a) foreign communications passed by wire, radio and other electromagnetic means . . . and (b) of selected foreign communications sent by non-electromagnetic means." *Id*. at ap. A.

22. It further defines "foreign communications" as "[c]ommunications of the Government, or of any military, air or naval forces, faction, party, department, agency or bureau of a foreign country, or of any person or persons acting or purporting to act therefor, and shall include [REDACTED] communications originated by nationals of a foreign country which may contain information of value." *Id.*

23. The 1955 UKUSA Agreement provides for the parties to "exchange" the "products" of "operations relating to foreign communications," including the "collection of traffic," "acquisition of communications documents and equipment," "traffic analysis," "cryptanalysis," and "decryption." *Id*. at ¶ 4(a). It further provides for the parties to "exchange . . . information regarding methods and techniques involved in the operations" relating to foreign communications. *Id.* at ¶ 5(a).

24. For the exchange of foreign communications "products," the 1955 UKUSA 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." *Id.* at ¶ 4(b). For the exchange of "methods and techniques," the Agreement provides that "[s]uch exchange will be unrestricted on all work undertaken except that upon notification of the other party information may be withheld by either party when its special interests so require" and that "[i]t is the intention of each party to limit such exceptions to the absolute minimum." *Id.* at ¶ 5(b). The Agreement also provides, in an appendix articulating

"General Principles of Collaboration on COMINT Production and Collection," that "[t]he objects of these arrangements is to ensure that maximum advantage is obtained from the combined available personnel and facilities of both parties." *Id.* at ap. C ¶ 2. The appendix further states 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." *Id.* at ap. C ¶ 3. 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." *Id*. at ap. H ¶ 1.

25. The 1955 UKUSA Agreement indicates that "[a]rrangements involving COMINT collection and production shall be established by agreement between Directors NSA and GCHQ" and that such arrangements "will implement the UKUSA Agreement." *Id.* at ap. C ¶ 1. The arrangements implementing the 1955 UKUSA Agreement have not been publicly disclosed.

The Evolution of Communications Technology and Surveillance

26. Methods of communication have dramatically changed since 1955. 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.

27. Many individuals today live major portions of their lives online. They use the internet to communicate with others, impart ideas, conduct research, explore their sexuality, seek medical advice and treatment, correspond with lawyers, and express their political and personal views. They also increasingly use the internet to conduct many ordinary activities, such as keeping records, arranging travel, and carrying out financial transactions. Today, much of this activity is conducted on mobile digital devices such as cellular phones, which "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

28. The internet has also enabled the creation of greater quantities of personal data about communications, known as "metadata." Metadata is information about a communication, which may include the sender and recipient, the date and location from where it was sent, and the type of device used to send it. Metadata can reveal web browsing activities, which might reveal medical conditions, religious viewpoints, or political affiliations. It can also reveal items purchased, news sites visited, forums joined, books read, movies watched and games played.

29. Communications – emails, instant messages, calls, social media posts, web searches, requests to visit a website – that utilize the internet can take any viable route to their destination; distance is not a determinative factor. They have the potential to travel around the world before reaching their destination, even if the information is being sent between two people (or a person and an entity) within a single country, or even a single city. 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.

30. The nature of signals intelligence has also changed dramatically since 1955. As modern communications have evolved, intelligence agencies have developed more advanced ways to access, acquire, store, analyze and disseminate this information. In particular, they have developed methods for acquiring communications and data transiting the internet. The costs of storing this information have decreased drastically and continue to do so every year. At the same time, technology now permits revelatory analyses of types and amounts of data that were previously considered meaningless or incoherent. Metadata, in particular, is structured in such a way that computers can search through it for patterns faster and more effectively than similar searches through the content of communications. Finally, the internet has facilitated remote access to information, meaning communications and data no longer need to be physically transferred from sender to recipient.

Prior Disclosures Concerning Five Eyes Surveillance

31. Over the last few years, information about the nature and scope of the surveillance conducted pursuant to the Five Eyes alliance has been disclosed to the public. The media has revealed, for example, that the NSA, together with its British counterpart GCHQ, acquired the contact lists and address books from hundreds of millions of personal email and instant-messaging accounts as well as webcam images from video chats of millions of Yahoo users. Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, Wash. Post (Oct. 14, 2013), http://wapo.st/2stOyAI.; Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, The Guardian (Feb. 28, 2014), https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo. It has further revealed that the two agencies have cooperated to tap and extract data from the

private fiber optic cables respectively connecting Yahoo and Google data centers, which are located around the world. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post (Oct. 30, 2013), http://wapo.st/1UVKamr.

32. The media has disclosed that, in addition to joint surveillance operations, the Five Eyes countries also grant each other broad access to the signals intelligence they each gather. For instance, it has revealed that the NSA has access to data flowing through undersea cables that land in the U.K. and intercepted by GCHQ and that GCHQ has access to a database containing the content and metadata of hundreds of millions of text messages collected by the NSA. Ewen MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, The Guardian (June 21, 2013), https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, The Guardian (Jan. 16, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep. It has further revealed that the Five Eyes countries each have access to a network of servers storing information acquired under various programs operated by their respective intelligence agencies. Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet*,' The Guardian (Jul. 31, 2013), https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; Morgan Marquis-Boire Et. Al., *XKeyscore: NSA's Google for the World's Private Communications*, The Intercept (July 1, 2015), https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/.

33. In recent years, the discussion of the government's foreign surveillance powers has focused primarily on the limitations imposed by several statutes, in particular, the Foreign Intelligence Surveillance Act ("FISA"), Section 215 of the Patriot Act (which expired in 2015), and the FISA Amendments Act of 2008. The discussion has also touched upon, to a lesser degree, the government's foreign surveillance powers pursuant to Executive Order 12,333 and the rules that regulate the government's acquisition, storage, analysis and dissemination of the communications of Americans pursuant to that surveillance. Little to no attention has been paid to the Five Eyes alliance and what rules govern the government's access to and acquisition, storage, analysis and dissemination of Americans' communications as part of that arrangement. Equally, little to no attention has been paid to what rules govern the government's exchange of signals intelligence it has acquired, stored and/or analyzed with the other members of the Five Eyes alliance.

The Current UKUSA Agreement

34. The 1955 revision is the most recent version of the UKUSA Agreement to have been made public. Over the past six decades, the NSA has disclosed no further documents relating to the UKUSA Agreement, including any subsequent revisions to the 1955 version of the Agreement.

35. The 1955 version of the UKUSA Agreement acknowledged that a reappraisal of the 1946 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."

36. Three parties to the 1955 UKUSA Agreement—the U.K., 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. *See* International Partners: How Sharing Knowledge and Expertise with Other Countries Helps Us Keep the UK Safe, GCHQ (Sept. 29, 2016), https://www.gchq.gov.uk/features/ international-partners; UKUSA Allies, Australian Signals Directorate, *available at* https://www.asd.gov.au/partners/ allies.htm; UKUSA Allies, Government Communications Security Bureau (December 6, 2016), https://www.gcsb.govt.nz/about-us/ukusa-allies/.

37. Upon information and belief, the UKUSA Agreement has been altered, amended, and/or extended many times since 1955.

38. Upon information and belief, since 1955 Defendants have adopted and/or created regulations, policies, legal opinions, and implementing documents, among other records, that constitute their statements of policy and interpretations of the UKUSA Agreement.

39. Upon information and belief, since 1955 Defendants have adopted and/or created strategy documents, directives, definitions, and technical manuals, among other records, that concern the implementation of the UKUSA Agreement and that constitute administrative staff manuals and instructions to staff that affect members of the public.

40. Defendants have failed to disclose publicly these statements of policy, interpretations, staff manuals, or instructions.

41. Any revisions to the UKUSA Agreement since 1955 also remain secret.

42. The public has no way of assessing whether the currently operative terms of the UKUSA Agreement contain sufficient constraints against the access to and acquisition, storage, analysis and dissemination of signals intelligence to satisfy domestic or international law.

43. Disclosing the currently operative provisions in the UKUSA Agreement for protecting privacy and Defendants' interpretations of those provisions is manifestly in the public interest. To the extent that the Agreement currently contains sufficient safeguards to protect privacy, the public will benefit from knowing that their rights remain protected. Should the Agreement lack such safeguards, the public will be able to demand change from their relevant executive officers.

The Requested Records

44. By letter dated December 13, 2016, Privacy International filed substantially similar FOIA requests with defendants NSA, ODNI, and State, and by letter dated March 16, 2016, Privacy International filed a substantially similar FOIA request with defendant NARA (the "Requests"). Those Requests sought disclosure of:

> 1. Any records governing, amending, extending or appended to the UKUSA Agreement.
>
> 2. Any records relating to the implementation of the UKUSA Agreement by the United States government, including, but not limited to:
>
> a. Regulations, policies, memoranda, legal opinions, strategy documents, directives, definitions, and technical manuals or specifications;
>
> b. Records pertaining to planning, technical and other relevant conferences, including, but not limited to, minutes, reports and recommendations.
>
> 3. Any records construing or interpreting the authority of the [agency] pursuant to the UKUSA Agreement; any regulations, policies or other implementing

documents issued thereunder; or any other relevant authorities pertaining to the UKUSA Agreement.

4. Any records describing the standards that must be satisfied for the "exchange" of "products" of "operations relating to foreign communications," as the [agency] defines these terms, pursuant to the [agency]'s authority under the UKUSA Agreement; any regulations, policies or other implementing documents issued thereunder; or any other relevant authorities governing the "exchange" of intelligence "products" under the UKUSA Agreement.

5. Any records describing the minimization procedures used by the [agency] with regard to the "exchange" of "products" of "operations relating to foreign communications," as the [agency] defines these terms, pursuant to the [agency]'s authority under the UKUSA Agreement; any regulations, policies or other implementing documents issued thereunder; or any other relevant authorities governing the "exchange" of intelligence "products" under the UKUSA Agreement.

6. Any other records governing the exchange of intelligence between the United States government and the governments of the United Kingdom, Canada, Australia and/or New Zealand.

True and correct copies of the Requests are collectively annexed hereto as Exhibit B, and incorporated by reference herein.

45. In its FOIA requests, Privacy International also sought a waiver of search, review, and duplication fees because the requested records were not sought for commercial use, Privacy International is a "representative of the news media" under 5 U.S.C. § 552(a)(4)(A)(ii)(II), and

the requested information is in the public interest as defined under 5 U.S.C. § 552(a)(4)(A)(iii).

Defendants' Treatment of Plaintiff's FOIA Requests

NSA

46. By letter dated December 27, 2016, NSA stated that, due to "delays in processing," it had not yet begun processing Privacy International's Request. The NSA further explained that it would not address Privacy International's request for a fee waiver until "further processing is done."

47. By letter dated February 24, 2017, Privacy International, through counsel, appealed NSA's constructive denial of Privacy International's Request (the "First NSA Appeal").

48. By letter dated April 24, 2017, John R. Chapman, Chief of the FOIA/PA Office, denied Privacy International's FOIA Request, asserting that all the records responsive to the FOIA Request were exempt from disclosure.

49. By letter dated May 31, 2017, Privacy International, through counsel, timely appealed the NSA's decision to withhold the requested documents (the "Second NSA Appeal").

50. By letter dated June 13, 2017, the NSA acknowledged Privacy International's appeal, assigned Plaintiff with an appeal case number, and stated that it would not comply with the appeal within the required statutory timeframe.

51. As of the filing of this Complaint, Privacy International has received no further information or communication from the NSA concerning the NSA Request or the First or Second NSA Appeals.

52. As of the filing of this Complaint, it has been 204 days since the Request was submitted, 131 days since the First NSA Appeal was submitted, and 35 days since the Second NSA Appeal was submitted.

ODNI

53. By letter dated January 11, 2017, ODNI informed Privacy International that it had initiated a search for the records requested. In that letter, ODNI granted Privacy International's request for a fee waiver.

54. By letter dated February 24, 2017, Privacy International, through counsel, appealed ODNI's constructive denial of Privacy International's Request.

55. As of the filing of this Complaint, Privacy International has received no further information or communication from the ODNI concerning the ODNI Request.

56. As of the filing of this Complaint, it has been 204 days since the Request was submitted, and 131 days since the appeal was submitted.

STATE

57. By letter dated December 14, 2016, State notified Privacy International that it was going to begin processing Privacy International's Request, and that the request for a fee waiver had been granted.

58. By letter dated February 24, 2017, Privacy International, through counsel, appealed State's constructive denial of Privacy International's Request.

59. By email dated March 8, 2017, Privacy International received a response from Jeanne Miller, Branch Chief at State, acknowledging the Request and the administrative appeal. Ms. Miller notified Privacy International that State was in the process of conducting a search for responsive records but had not located any to date.

60. By letter dated April 6, 2017, Lori Hartmann, Appeals Officer at State's Office of Information Programs and Services, denied Privacy International's appeal on the basis that the Request had not been denied and was still being processed.

61. By email dated May 18, 2017, Privacy International received a response from Ms. Miller indicating that the FOIA Request would be "administratively closed" unless Privacy International responded within twenty days.

62. By email dated May 19, 2017, Privacy International, through counsel, responded, indicating that State should continue to process the Request and search for responsive records.

63. As of the filing of this Complaint, Privacy International has received no further information or communication from State concerning the State Request.

64. As of the filing of this Complaint, it has been 204 days since the Request was submitted and 90 days since the appeal was denied.

NARA

65. By email dated March 16, 2017, NARA sent Privacy International an automated response confirming its receipt of Privacy International's Request and explaining that it had forwarded the Request to the "Office of Research Services, Special Access and FOIA" division. NARA additionally stated that Privacy International would be assigned a new tracking number.

66. As of the filing of this Complaint, Privacy International has not received a tracking number for its Request.

67. As of the filing of this Complaint, Privacy International has received no further information or communication from NARA concerning the NARA Request.

68. As of the filing of this Complaint, it has been 111 days since the Request was submitted.

69. None of the four Defendant agencies has produced any records responsive to Privacy International's Requests.

CAUSES OF ACTION

Count I

Violation of FOIA for wrongful withholding of agency records

70. Plaintiff repeats, re-alleges, and incorporates the allegations in the foregoing paragraphs as though fully set forth herein.

71. Defendants are agencies subject to FOIA. 5 U.S.C. § 556(f); 5 U.S.C. § 551. The FOIA Requests properly seek records within the possession, custody, and/or control of Defendants.

72. Defendants' failure to make available the records requested by Plaintiff in a timely manner violates FOIA. 5 U.S.C. § 552(a)(3)(A).

73. Plaintiffs have or are deemed to have exhausted applicable administrative remedies. 5 U.S.C. § 552(a)(6)(C)(i).

Count II

Violation of FOIA by NSA and NARA for failure to grant fee waiver

74. Plaintiff repeats, re-alleges, and incorporates the allegations in the foregoing paragraphs as though fully set forth herein.

75. Defendants NSA and NARA's failure to grant Plaintiff's request for a public interest fee waiver violates FOIA. 5 U.S.C. § 552(a)(4)(A)(iii).

Count III

Violation of FOIA for failure to make records available under "Reading Room" provision

76. Plaintiff repeats, re-alleges, and incorporates the allegations in the foregoing paragraphs as though fully set forth herein.

77. Defendants have failed to make available for public inspection in an electronic format their statements of policy and interpretations concerning the UKUSA Agreement, which they have adopted and not published in the Federal Register, and all administrative staff manuals and instructions to staff concerning the UKUSA Agreement that affect a member of the public.

78. Defendants' failure to make available for public inspection in an electronic format their statements of policy and interpretations of the UKUSA Agreement, staff manuals and instructions violates FOIA, 5 U.S.C. § 552(a)(2).

RELIEF REQUESTED

WHEREFORE, Plaintiff respectfully requests this Court to:

a. Declare that Defendants have failed to comply with the disclosure obligations of 5 U.S.C. 552(a)(3);

b. Order Defendants to conduct a thorough search for all records responsive to Plaintiff's Requests and to immediately disclose, in their entirety, all responsive records that are not specifically exempt from disclosure under FOIA;

c. Declare that Defendants have failed to comply with the disclosure obligations of 5 U.S.C. 552(a)(2);

d. Order Defendants to make available for public inspection in an electronic format those responsive documents that constitute statements of policy

and interpretations of the UKUSA Agreement, which have been adopted by the agency and are not published in the Federal Register;

e. Order Defendants to make available for public inspection in an electronic format those responsive documents that constitute staff manuals and instructions concerning the UKUSA Agreement that affect a member of the public;

f. Declare that Plaintiff is entitled to a public interest fee waiver;

g. Award Plaintiff the costs of this proceeding, including reasonable attorneys' fees and costs; and

h. Grant such other and further relief as the Court deems just and proper.

Dated: July 5, 2017

Respectfully submitted,

YALE LAW SCHOOL MEDIA FREEDOM AND INFORMATION ACCESS CLINIC

By: */s/ Hannah Bloch-Wehba*

Hannah Bloch-Wehba (Bar ID 1031703)
Media Freedom and Information Access Clinic
Yale Law School
P.O. Box 208215
New Haven, CT 06520-8215
Tel: (203) 436-5824
Fax: (203) 432-3034
hannah.bloch-wehba@yale.edu

David A. Schulz (Bar ID 459197)
321 West 44th Street, Suite 1000
New York, NY 10036
Tel: (212) 850-6100
Fax: (212) 850-6299
dschulz@lskslaw.com

Counsel for Plaintiff

Of Counsel:
Scarlet Kim
Caroline Wilson Palow
Privacy International
62 Britton Street
London, EC1M 5UY
United Kingdom
Tel: +44 (0) 20 3422 4321
scarlet@privacyinternational.org
caroline@privacyinternational.org

2783

~~TOP SECRET~~

LSIB/141/55.

10th May, 1955.

Copy No. 48

AMENDMENT NO. 4 TO THE APPENDICES

TO THE UKUSA AGREEMENT

(THIRD EDITION)

Please add the following Note after paragraph 16 of the Introduction to the UKUSA Appendices (dated 1st June 1951):

"On 1st May 1955 USCIB and LSIB agreed that a general revision of the Appendices was required. They further agreed that as a first step toward such revision USCIB would furnish LSIB, for comment, detailed proposals which are being prepared by USCIB. Pending agreement by both parties on a general revision of the Appendices, the Directors, NSA and GCHQ will:

(a) determine jointly any changes which may be required in Appendices C, D, E, F, K, L, and M and

(b) implement any such changes which they agree to be necessary.

Although this interim authorization enables the Directors, NSA and GCHQ, to change or interpret specified Appendices by mutual agreement, it does not require USCIB or LSIB to approve such changes or interpretations provided these are within the spirit and intent of current UKUSA policy."

Secretary,
Sigint Board.

~~TOP SECRET~~

TOP SECRET

TO BE HANDLED IN ACCORDANCE WITH IRSIG

EIDER

Ref. [redacted]

TOP SECRET EIDER

10th October, 1956.

Director. (Copies to: [redacted]

UKUSA Agreement

Attached are copies of the UKUSA Agreement and its policy appendices as now informally agreed between the representatives of NSA and GCHQ. NSA will now reconsider these papers and will then submit them to USCIB for the latter to propose formally to LSIB.

2. The factors affecting the need for a reappraisal of the Agreement at this time are:-

(a) the setting up and development of NSA and the defining of the responsibilities of Director, NSA; this has led to a similar relationship between Director, NSA and USCIB as existed between Director, GCHQ and LSIB;

(b) the passage of time which has made out of date much of the detail contained in the Agreement.

3. The work in preparing these papers has been done on the basis of

(a) making a separation as between the technical and the policy material contained in the basic Agreement and the appendices, and

(b) so redrafting the basic Agreement and the policy appendices that they contain all the matter which is the province of the two Boards leaving all technical matters for mutual agreement between the Directors of GCHQ and NSA.

4. The following are the salient points affecting the papers as now revised:-

A. The Agreement

(a) It was agreed that it would be preferable to amend the old Agreement rather than to negotiate a new Agreement. The changes made have been kept to the minimum practicable.

(b) The modernisation of the first paragraph of the Agreement commits the US and the UK as a whole and not only the organisations represented on the two Boards.

(c) Paragraph 3 is new and has been inserted to define the status of the policy appendices as integral parts of the basic Agreement.

B. Appendix A.

(a) The new appendix A contains considerably fewer definitions since only such definitions as are required for the

[redacted]tation

interpretation of the Agreement and its policy appendices have been included. Such other definitions as may be required for the interpretation of the technical working documents to be agreed between Directors, NSA and GCHQ will form an integral part of each such document.

(b) The definition of SIGINT refers to both COMINT and ELINT, but GCHQ has agreed to the NSA preference not to make the definition of ELINT a separate heading.

C. Appendix B.

Comparatively minor changes have been agreed at this stage to meet NSA's wish to avoid raising any controversial issue affecting categorisation which is now under detailed review in USCIB.

D. Appendix C.

The new Appendix C covers what is appropriate to the Boards of the old appendices D, E and F and most of the old Introduction to the appendices.

E. Appendix I.

The new Appendix I has been so drafted as to make clear the distinction between the Senior Liaison Officers in both countries who are appointed by and accredited to the two Boards and other liaison personnel and COMINT specialists appointed by the Directors, NSA and GCHQ to meet their own requirements. (There is a possibility that SUSLO may at a later stage not report to Director, NSA).

F. Appendix H.

The new Appendix H has been so drafted that the detailed content of the annexures to the old appendix become specifically the responsibility of the Directors, NSA and GCHQ.

G. Appendix N.

The new paragraph 3 of this Appendix has been so drafted that it may correctly reflect both the rather wider responsibilities of Director, NSA and also the co-ordinating function of Director, GCHQ in this context.

H. Appendix Q.

The new Appendix Q is now a statement of the general principles of war-time co-operation and the detailed planning based in the pre-1954 concept of global war which was contained in the old appendix has all been omitted, including that for the CCE. It was agreed that when present planning activity reaches the point where mutual discussions may be fruitful, plans corresponding to the post-1954 concept should be set up, but as NSA/GCHQ documents.

/5.

5. NSA/GCHQ agreement of the new technical working documents.

(a) On the question of how, in future, to record the technical agreements between the Directors, NSA and GCHQ it was agreed that no attempt should be made to over-formalise and that the present direct exchanges of signals and letters should continue. Nevertheless, some series of documents would be advisable, with the devolution of responsibility for blocks within the series to corresponding parts of NSA and GCHQ. Typical blocks would be:-

Research crypt	(H)
T/A data	(J and K)
Division of cover	(S)
Reporting policy	(Z)

(b) Aspects of the old appendices D, E, F, O, H and the whole of appendices K, L and M will all have to be considered for inclusion in this series of technical documents. At some stage in the official exchanges between the Boards it will need to be recorded that these remain in force until agreed otherwise by the two Directors.

Z

W

U.K. - U.S. COMMUNICATIONS INTELLIGENCE AGREEMENT (UKUSA AGREEMENT)

1. Parties to the Agreement

The following agreement is made between the United States Communications Intelligence Board (USCIB) (formerly known as STANCIB, representing the U.S.) and the London Signal Intelligence Board (LSIB) (representing the U.K.).

2. Scope of Agreement

The agreement governs the relations of the above-mentioned parties in communications intelligence (hereinafter referred to as COMINT) matters only. However the exchange of such collateral material as is applicable for technical purposes and is not prejudicial to national interests will be effected between the National Communication Intelligence Agencies of both countries.

3. Appendices to the Agreement

Certain terms used in the Agreement are defined in Appendix A. Additional documents are appended for the purpose of clarifying the agreement, stating the principles of COMINT security, and otherwise guiding or governing the collaboration between the two countries in COMINT matters. The appendices are described more fully in an introduction to the appendices (attached hereto).

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.

/(b)

(b) Such 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. It is the intention of each party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon.

5. Extent of the Agreement - Methods and Techniques

(a) The parties agree to the exchange of information regarding methods and techniques involved in the operations outlined in paragraph 4(a).

(b) Such exchange will be unrestricted on all work undertaken except that upon notification of the other party information may be withheld by either party when its special interests so require. Such notification will include a description of the information being withheld, sufficient in the opinion of the withholding party, to convey its significance. It is the intention of each party to limit such exceptions to the absolute minimum.

6. Third Parties to the Agreement

Both parties will regard this agreement as precluding action with third parties on any subject appertaining to COMINT except in accordance with the following understanding:-

(a) It will be contrary to this Agreement to reveal its existence to any third party unless otherwise agreed by the two parties.

(b) Except as laid down in Appendix P, each party will seek the agreement of the other to actions with third parties, and will take no such action until its advisability is agreed upon.

(c) The agreement of the other having been obtained, it will be left to the party concerned to carry out the agreed action in the most appropriate way, without obligation to disclose precisely the channels through which action is taken.

/(d)

(d) Each party will ensure that the results of any of its actions with third parties are made available to the other.

7. Commonwealth Countries other than the U.K.

(a) While Commonwealth Countries other than the U.K. are not parties to this agreement, they will not be regarded as third parties.

(b) LSIB will keep USCIB informed of any arrangements or proposed arrangements with other Commonwealth COMINT Authorities.

(c) USCIB will make no arrangements in the sphere of COMINT with any Commonwealth COMINT Authorities other than Canadian, except through, or with the prior approval of, LSIB.

(d) As regards Canada, USCIB will complete no arrangements with any COMINT Authority therein, without first obtaining the views of LSIB.

(e) It will be conditional on any Commonwealth Authorities with whom collaboration takes place that they abide by the terms of paragraphs 6, 9 and 10 of this agreement and by the arrangements laid down in paragraph 8.

8. Arrangements between LSIB and U.S. Authorities and USCIB and U.K. Authorities

(a) LSIB will make no arrangements in the sphere of COMINT with any U.S. authority except through, or with prior approval of, USCIB.

(b) USCIB will make no arrangements in the sphere of COMINT with any U.K. authority except through, or with prior approval of, LSIB.

9. Dissemination and Security

Classified COMINT information and materials will be disseminated and safeguarded in accordance with principles drawn up and kept under review by USCIB and LSIB in collaboration. These principles shall be the basis for all regulations on this subject issued by or under the authority of USCIB or LSIB and other appropriate authorities of the Governments of the two parties. Within the terms of these regulations dissemination by either party will be made to U.S.

recipients only as approved by USCIB; to Commonwealth recipients other than Canadian, only as approved by LSIB; to Canadian recipients only as approved by either USCIB or LSIB; and to third party recipients only as jointly approved by USCIB and LSIB as provided in Appendix P.

10. Dissemination and Security - Commercial

USCIB and LSIB will ensure that without prior notification and consent of the other party in each instance no dissemination of information derived from COMINT sources is made to any individual or agency, governmental or otherwise, that will exploit it for commercial purposes.

11. Previous Agreements

This Agreement supersedes all previous Agreements between U.K. and U.S. authorities in the COMINT field.

12. Amendment and Termination of Agreement

This Agreement may be amended or terminated completely or in part at any time by mutual agreement. It may be terminated completely at any time on notice by either party, should either consider its interests best served by such action.

13. Activation and Implementation of Agreement

This Agreement becomes effective by signature of duly authorized representatives of the parties. Thereafter, its implementation will be arranged between the COMINT authorities concerned subject to the approval of LSIB and USCIB.

For and in behalf of the
London Signal Intelligence Board

For and in behalf of the United States
Communications Intelligence Board

/Introduction to

INTRODUCTION TO THE APPENDICES TO

THE UKUSA AGREEMENT

1. The following is a list of documents which were attached to, and considered integral parts of, the UKUSA Agreement at the time of its amendment:-

(a) This Introduction.

(b) Appendix A, Definitions of Certain Terms Used in the UKUSA Agreement.

(c) Appendix B, Principles of Security and Dissemination.

(d) Appendix C, General Principles of Collaboration between COMINT Agencies.

(e) Appendix G, Exchange of Collateral Material and COMINT Material which is obtained [redacted]

OGA
EO 1.4.(c)
EO 1.4.(d)

(f) Appendix H, Communications.

(g) Appendix I, Liaison and Methods of Communication.

(h) Appendix J, Principles of UKUSA Collaboration with Commonwealth Countries, other than the U.K.

(i) Appendix N, Emergency Planning.

(j) Appendix P, COMINT Relations with Third Parties.

(k) Appendix Q, COMINT Collaboration in War.

2. The object of the appendices is to clarify the basic agreement by stating in some detail the principles of COMINT security and otherwise guiding or governing the collaboration between the two parties. Amendments to the appendices (including the addition of new appendices) will be made as required and agreed by USCIB and LSIB.

3. The technical aspects of COMINT collaboration, i.e. those which do not require the approval of LSIB or USCIB, will be arranged as required and agreed by the Director, NSA, and the Director, GCHQ. Such arrangements will be made in accordance with the principles of collaboration as set forth in the UKUSA Agreement. The object of these technical arrangements is to ensure that maximum advantage is obtained from the combined available facilities of both parties.

APPENDIX A

DEFINITIONS OF CERTAIN TERMS USED IN THE UKUSA AGREEMENT

British Commonwealth[*]

Collateral Material — Non-COMINT material which is of assistance in the collection or production of COMINT, or is otherwise applicable for technical COMINT purposes.

COMINT — The name given to all processes involved in, and intelligence information and technical material resulting from, the interception and study of (a) foreign communications passed by wire, radio and other electromagnetic means (except press, propaganda, and public broadcasts) and (b) of selected foreign communications sent by non-electromagnetic means.

COMINT Agency — A national COMINT collection and production authority, i.e. in the U.S. NSA, in the U.K. GCHQ.

COMINT Authority — An authority who is responsible for the collection, production, dissemination, or use of COMINT.

Foreign Communications — Communications of the Government, or of any military, air or naval forces, faction, party, department, agency or bureau of a foreign country, or of any person or persons acting or purporting to act therefor, and shall include [redacted] communications originated by nationals of a foreign country which may contain information of value.

OGA
EO 1.4.(c)
EO 1.4.(d)

/Signal

[*] USCIB proposes that this definition be drafted by LSIB.

Signal Intelligence (SIGINT)	Includes both COMINT and ELINT (ELINT is information obtained by intercepting and analyzing non-communications transmissions).
Foreign Country	Any country, whether or not its government is recognized by the U.S. or the U.K., excluding only the U.S. and The Commonwealth.
Technical Material	(1) Data concerning (a) cryptographic systems, (b) communications including procedures and methods, (c) methods used in the collection and production of COMINT, (d) equipment as used in or designed for COMINT processes; (2) information or material related to data of the types enumerated in (1) above.
Third Parties	All individuals or authorities other than those of the U.S. and The Commonwealth.

NOTE: Other Appendices to the UKUSA Agreement may contain certain terms having specialized meanings for the purpose of those appendices. In such cases the terms are defined in those appendices.

/Appendix B.

APPENDIX B

Para. 4 - (a) First sentence to read:-

"There are two types of COMINT end-product: Crypt Intelligence and Traffic Intelligence [See note 2]."

(b) "intelligence information" to be substituted for "COMINT" in subparas. a. and b.

Paras. 6 (b) and 7 - To be amended as may be finally agreed by USCIB and LSIB.

Paras. 12 and 13 - Amend second sentences to read (as recently agreed by USCIB and LSIB):-

"Such codewords shall be replaced when in the opinion of either USCIB or LSIB a requirement exists for a change."

Para. 31 - Insert after first sentence:

"In the case of Allied Commands involving the U.S. and the U.K., the level will be established for each command by agreement between USCIB and LSIB. It is understood that the responsibility thus assigned will be exercised over all subordinate U.S. and U.K. personnel. Exceptions shall be authorized only after careful consideration in each instance of the advantages to be gained, as opposed to the risk involved."

Para. 35d - Insert after second sentence:

"In the case of allied commands involving the U.S. and the U.K., the level will be established for each command by agreement between USCIB and LSIB."

Para. 35e - Insert after second sentence:

"In the case of allied commands involving the U.S. and the U.K., the level will be established for each command by agreement between USCIB and LSIB.

Para. 36a - Substitute:

"Whenever Category I COMINT is to be transmitted by a means exposed to interception, it shall normally be transmitted in an appropriate cryptographic system. When there is no suitable means of secure communication available, Category I COMINT classified CONFIDENTIAL may be transmitted in plain language if there is an urgent operational need to do so. Whenever possible such plain language transmission shall be in the form of operational orders so worded that the subject matter cannot be traced specifically to its

COMINT origin. Category I COMINT which may be classified higher than Confidential may not be transmitted in plain language by a means exposed to interception."

Para. 37b - Add to end of paragraph:

"In the case of allied commands involving the U.S. and the U.K., the level will be established for each command by agreement between USCIB and LSIB."

Para. 40b.(2) - Amend last sentence to read:-

"Similarly, the classification (and codeword) need not appear on every sheet of raw traffic and technical material passed between COMINT agencies and units."

Para. 45c. - Delete "mutually" in line 1.

Note 1 - To be deleted. Now absorbed in Appendix 'A'.

Note 2 - To be amended as may be finally agreed by USCIB and LSIB.

ANNEXURE B1

Paras. 3 and 5 - To be amended as may be finally agreed by USCIB and LSIB.

APPENDIX C

GENERAL PRINCIPLES OF COLLABORATION ON COMINT PRODUCTION AND COLLECTION

1. Arrangements involving COMINT collection and production shall be established by agreement between Directors NSA and GCHQ. These arrangements will implement the UKUSA Agreement and will take effect within the scope and limitations established thereby.

2. The object of these arrangements is to ensure that maximum advantage is obtained from the combined available personnel and facilities of both parties.

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*.

4. The conveyance by one agency or unit to another, pursuant to paragraphs 4a(2) and (6), and 5(a) of the UKUSA Agreement, of a device or apparatus, may take the form of a gift, loan, sale, rental or rendering available, as may be agreed and arranged by the agencies concerned in the specific instance. The fact that the disclosing agency may have the privilege of using a method or technique, or a device or apparatus pertaining thereto, on a royalty-free basis, shall not of itself relieve the receiving agency of the obligation to pay royalties.

---

*The channel for this exchange will be between the Directors NSA and GCHQ unless they agree otherwise.

/Appendix H.

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.

2. The Director, GCHQ and the Director, NSA will ensure that mutual COMINT communications problems are kept under review and will assist each other as may be required on such problems. They will ascertain communications requirements for collection and exchange, take the necessary steps to see that these communications are provided and keep each other informed of progress.

3. Installation, Maintenance and Operation of Terminals.

The terminals of circuits or channels intended exclusively to carry COMINT traffic between the British Commonwealth and the United States will be installed, maintained and operated as arranged by the appropriate COMINT authorities of the countries concerned, and, although normally such terminals will be installed, maintained and operated by the appropriate U.S. or British Commonwealth authority on whose territory the terminals are situated, this will not be obligatory.

4. Provision of Equipment

The provision of equipment of all types will be by mutual assistance where necessary and practicable and as agreed in each specific case.

5. Cryptographic Aids.

(a) Common cryptographic aids will be used for combined COMINT communications. The matter of cryptographic aids will be kept continuously under review with the object of maintaining and increasing securit[illegible] facilitating

facilitating communications.

(b) In order to reduce the number of personnel required for communication and cryptographic operations and thereby to augment the forces available for direct intercept operations, and also to improve speed and accuracy, the ultimate goal should be the transmission of all COMINT material in on-line cryptosystems. Every effort should be made towards this end, consistent with the policies of both countries.

6. Bag Routes

Bag routes will be kept under review with the object of taking full advantage of sea and air services.

7. Microfilm

Both Agencies will be equipped to handle microfilm so that it may be available for use when it is not practicable to send the original material.

/Appendix I.

APPENDIX I

LIAISON AND METHODS OF COMMUNICATION

LIAISON PERSONNEL

1. Each party shall maintain, in the country of the other, a senior liaison officer accredited to the other. Such officers shall be responsible each in the country to which he is accredited for all liaison matters.

2. The Directors, NSA and GCHQ, shall provide for additional liaison, as may be required between the agencies. All such additional liaison personnel shall be under the control and direction of the senior liaison officer. Upon agreement between the Directors, COMINT specialists may be assigned to agencies or units of either party by the other. In so doing, the Directors shall reach a mutually acceptable understanding on the control and direction of the COMINT specialists. Suitable office facilities will be made available as necessary by the agency to which liaison personnel are assigned.

3. Each party shall normally assist the other's senior liaison officer by making available to him facilities for packaging and preparing material for transportation. Each party shall, to the extent of facilities operated by or available to it, assist the other's senior liaison officer with safe-hand and other transportation within its own country.

4. Liaison officers of one party shall normally have unrestricted access to those parts of the other's agencies which are engaged directly in the production of COMINT, except such parts thereof which contain unexchangeable information. The points of contact of liaison officers within agencies for requests and enquiries shall be determined, established and delimited by the party to which they are accredited.

5. In addition to the above regularly assigned personnel, visits by selected personnel for short periods of time to deal with special problems will be encouraged.

/6.

COMMUNICATION VIA SENIOR LIAISON OFFICERS

6. The channel whereby either party communicates with the other shall be the sender's senior liaison officer. The receiving party shall respond to such action via the same liaison officer.

7. The provisions of paragraph 6 above shall not be construed as preventing either party from accommodating the other by transporting or communicating information or material for the other party.

/Appendix J.

APPENDIX J

ANNEXURE J1

Certain consequential amendments of the references to paragraphs in the Agreement will be necessary.

Paragraph 6 - Substitute:

"The direct collaboration and consequent exchanges between NSA and DSB will be regulated by pertinent provisions of Appendices C, G, H and I to the UKUSA Agreement, and by pertinent technical procedures which shall be established by NSA and GCHQ pursuant to Appendix C.

APPENDIX N

ARRANGEMENTS FOR EMERGENCY RE-LOCATION OF COMINT UNITS

APPENDIX Q

ORGANIZATION OF UKUSA COMINT COLLABORATION IN WAR

INTRODUCTION

1. The UKUSA Agreement (including its appendices) and the operating arrangements based thereon will continue to be the basis of relations between the two parties in war.

2. In interpretation of this agreement the general principles and considerations stated below provide for particular spheres of collaboration between the two parties during a war in which the U.S. and the U.K. are allied.

3. The aim of the two parties is to ensure that the greatest possible contribution consistent with security is made by their combined COMINT effort to the prosecution of a war.

PRINCIPLES OF COLLABORATION BETWEEN
COMINT AGENCIES OR UNITS IN WARTIME

4. Specific U.S. and U.K. requirements and capabilities regarding wartime collaboration between COMINT agencies or units shall be established. The Directors shall maintain in a mutually agreed form a detailed plan for such wartime collaboration. Insofar as practicable, phasing for implementing actions shall be indicated in the plan, including those actions which are in the nature of wartime preparations, and which must be initiated prior to the outbreak of hostilities. Consistent with each party's freedom to establish its own COMINT organization, and to undertake any task relevant to its national worldwide interests, the Directors, NSA and GCHQ, shall consider in their planning the necessity and feasibility of the following types of action:-

(a) A broad division of COMINT tasks between the U.S. and U.K. organizations.

(b) The augmentation of one party's resources by the supply of selected personnel and materiel from the other.

/(c)

(c) The integration of selected U.S. and U.K. organizations.

(d) The establishment of new channels for liaison or for the exchange of raw traffic, technical material, and end-product between selected U.S. and U.K. authorities.

(e) The assignment of working groups of one party to the other party's agencies or units.

(f) The participation by either party in the other's COMINT organizations, including the arrangements for operational, technical or administrative control, logistical support, and the establishment and maintenance of communications.

5. Planning for tactical Comint, 'Y' or close support constitutes a special case. Coordination of such planning within Allied Commands will be in accordance with Appendix P. Coordination of such planning outside Allied Commands will be in accordance with assigned national responsibilities.

810/1.

Directorate Minute Sheet.

~~TOP SECRET~~ ~~EIDER~~ Reference No.: D/7707.

6th January, 1955.

Subject: APPENDIX E TO UKUSA AGREEMENT.

(1) Attached is a revised version of Appendix E, effective as from 1st January 1955, which has been agreed between Directors, NSA and GCHQ. Further copies are available on request.

2. The existing Appendix E, dated 1st June 1951, is replaced by this new version, with immediate effect, but should not be destroyed pending formal USCIB-LSIB agreement on the revision.

K. A. Perrin

DA.

~~TOP SECRET~~ ~~EIDER~~

Referred to

OGA
EO 1.4.(d)

SUKLO Washington
Copy to: SUSLO (without enclosures).

After Action

810/1.

Directorate Minute Sheet.

W.

Amendment No.4 completed. 17.6.60.
Amendment No.5 completed 17/6/60.

~~TOP SECRET~~ EIDER

Reference No. D/0167.

5th July, 1956.

Subject: Amendments to Appendix E to UKUSA Agreement.

OGA
EO 1.4.(c)
EO 1.4.(d)

~~TOP SECRET~~ EIDER

APPENDIX E

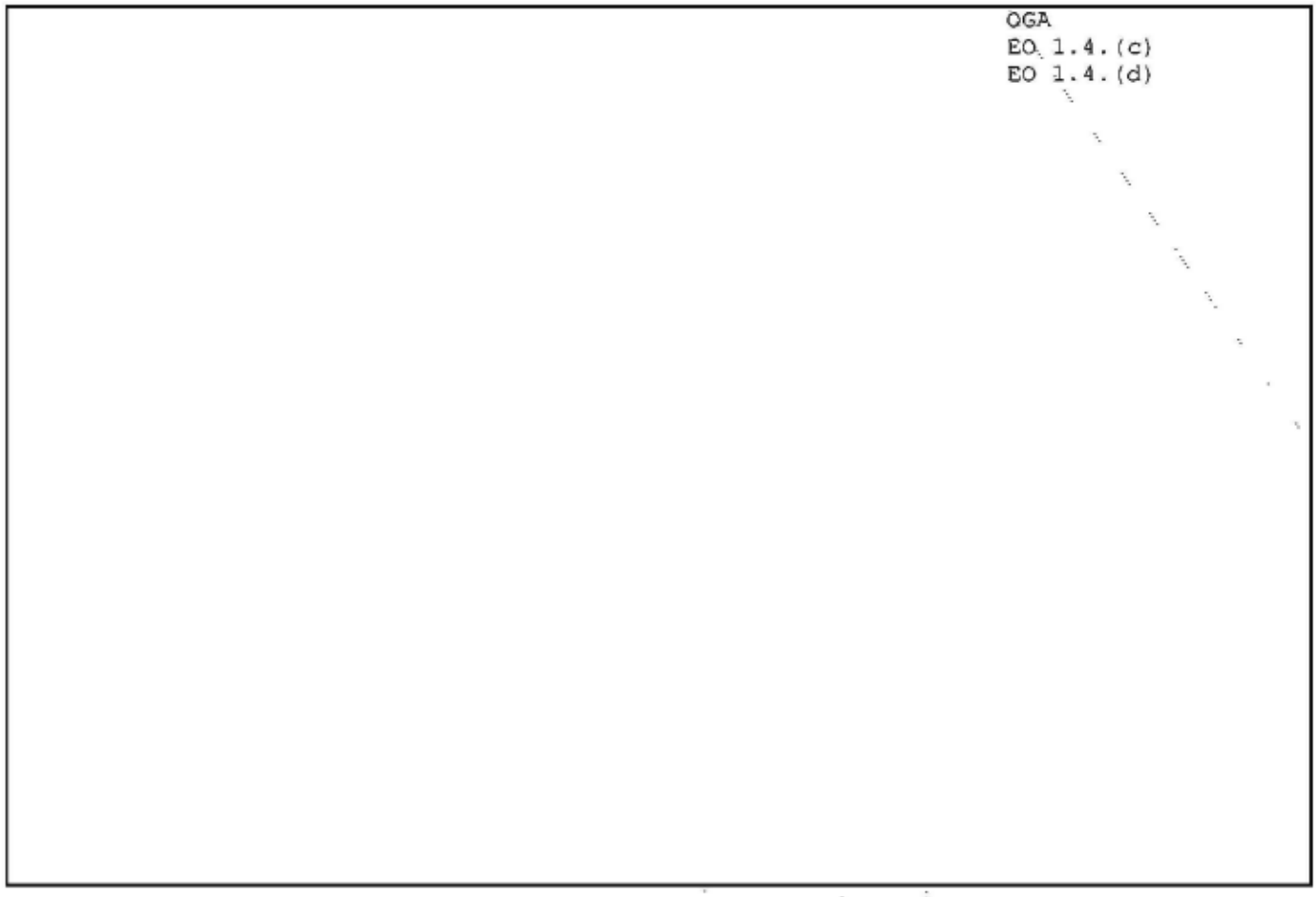
CO-ORDINATION OF, AND EXCHANGE OF INFORMATION ON, CRYPTANALYSIS AND ASSOCIATED TECHNIQUES

ALLOCATION OF TASKS

1. Allocation of major tasks, conferring a one-sided responsibility, is undesirable and impracticable as a main principle; however, in order that the widest possible cover of foreign cypher communications be achieved, the Comint Agencies of the two parties shall exchange proposals for the elimination of duplication. In addition, collaboration between those Agencies will take the form of suggestion and mutual arrangement as to the undertaking of new tasks and changes in status of old tasks.

2. Notwithstanding any informal allocations based on the above, all raw traffic shall continue to be exchanged except in cases where one or the other party agrees to forgo its copy.

OGA
EO 1.4.(c)
EO 1.4.(d)


OGA
EO 1.4.(c)
EO 1.4.(d)

OGA
EO 1.4.(c)
EO 1.4.(d)

APPENDIX E

OGA
EO 1.4.(c)
EO 1.4.(d)

OGA
EO 1.4.(c)
EO 1.4.(d)

TABLE B (contd.)

OGA
EO 1.4.(c)
EO 1.4.(d)

APPENDIX E

OGA
EO 1.4.(c)
EO 1.4.(d)

APPENDIX H

COMMUNICATIONS

(For details See Annexure H1)

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 the rapid flow of all types of raw traffic from the points of interception to the several Agencies; the rapid exchange of all types of raw traffic, technical matter and Communication Intelligence between the Agencies; and the efficient control of interception coverage. In addition lateral communications between stations of one party and Agencies or stations of the other may be provided for the same purposes as necessary and mutually agreed.

2. INSTALLATION, MAINTENANCE AND OPERATION OF TERMINALS

The terminals of circuits or channels intended exclusively to carry Comint traffic between the British Commonwealth and the United States will be installed, maintained and operated as arranged by the appropriate Comint Authorities of the countries concerned and, although normally such terminals will be installed, maintained and operated by the appropriate U.S or British Commonwealth authority on whose territory the terminals are situated, this will not be obligatory.

3. PROVISION OF EQUIPMENT

The provision of equipment of all types will be by mutual assistance where necessary and practicable and as agreed in each specific case.

4. CRYPTOGRAPHIC AIDS

(a) Common cryptographic aids will be used for combined Comint Communications. The matter of cryptographic aids will be kept continuously under review with the object of maintaining and increasing security and of facilitating communications.

(b) In order to reduce the number of personnel required for communication and cryptographic operations and thereby to augment the forces available for direct intercept operations, and also to improve speed and accuracy, the ultimate goal should be the transmission of all Comint material in on-line cryptosystems. Every effort should be made towards this end, consistent with the policies of the services of both countries.

5. BAG ROUTES

Bag routes will be kept under review with the object of taking full advantage of sea and air services.

6. MICROFILM

All agencies will be equipped to handle microfilm so that it may be available for use when it is not practicable to send the original material.

7. COMMUNICATIONS LIAISION

A representative of the Director, GCHQ, and a representative of the Director, National Security Agency, will be given the specific duty of keeping under review Comint communications problems and of raising and advising on such problems as they occur.

8. COMMUNICATION REQUIREMENTS IMPOSED BY OTHER APPENDICES

It is agreed that when all appendices which impose a communication requirement are approved by Comint authorities of all parties to the proposed Comint Conference, the communications annexures appended thereto will be included in Appendix H and made object of such action as is necessary to fulfill their requirements.

~~TOP SECRET - SECURITY INFORMATION~~

OGA
EO 1.4.(c)
EO 1.4.(d)

APPENDIX H
Annexure H_1 - sheet 1

APPENDIX H

ANNEXURE H_1

WORKING ARRANGEMENTS REACHED AT THE 1953 CONFERENCE FOR THE IMPLEMENTATION OF APPENDIX H (COMMUNICATIONS)

[redacted]

TOP SECRET COMINT, 53-7(a)
COPY 100 OF 114 COPIES
PAGE 4 OF 15 PAGES

TOP SECRET

APPENDIX H
Annexure H1 - sheet 2

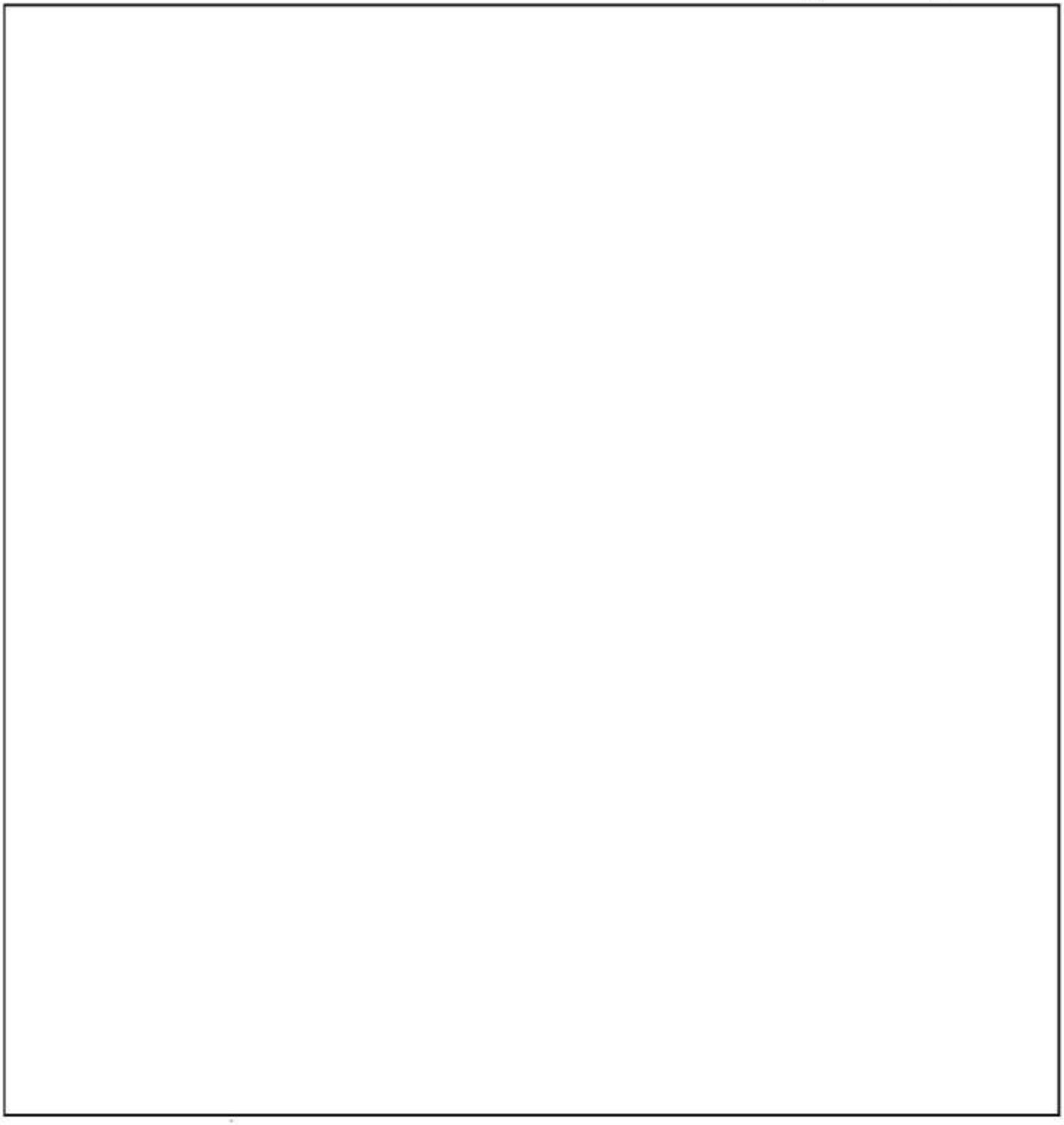
OGA
EO 1.4.(c)
EO 1.4.(d)

OGA
EO 1.4.(c)
EO 1.4.(d)

~~TOP SECRET~~

~~TOP SECRET~~

APPENDIX H
Annexure H_1 = sheet 3

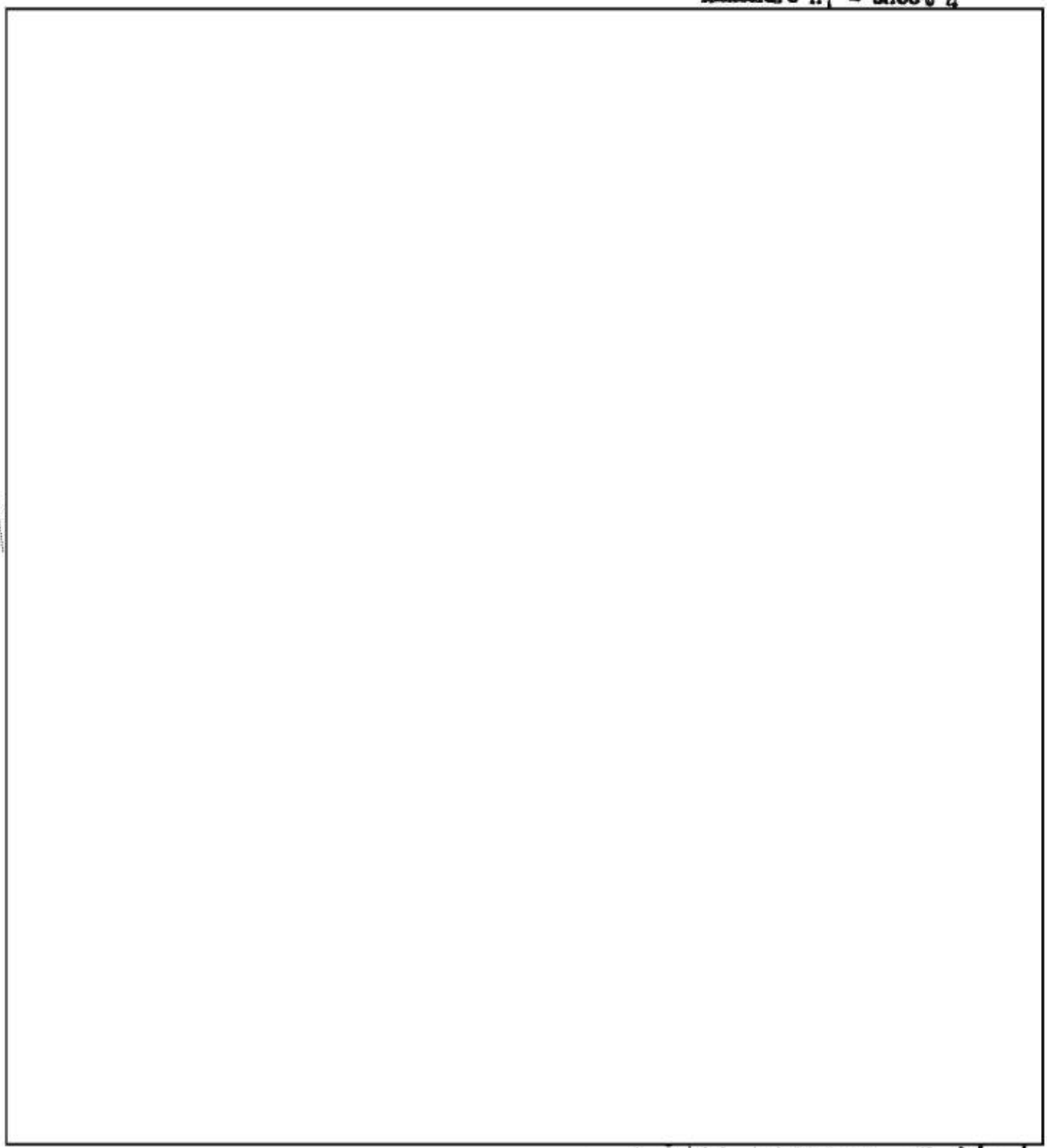


TOP SECRET CONTROL NUMBER 53-7(w).
COPY 100 OF 114 COPIES
PAGE 6 OF 15 PAGES

~~TOP SECRET~~

~~TOP SECRET~~

APPENDIX H
Annexure H_1 - sheet 4



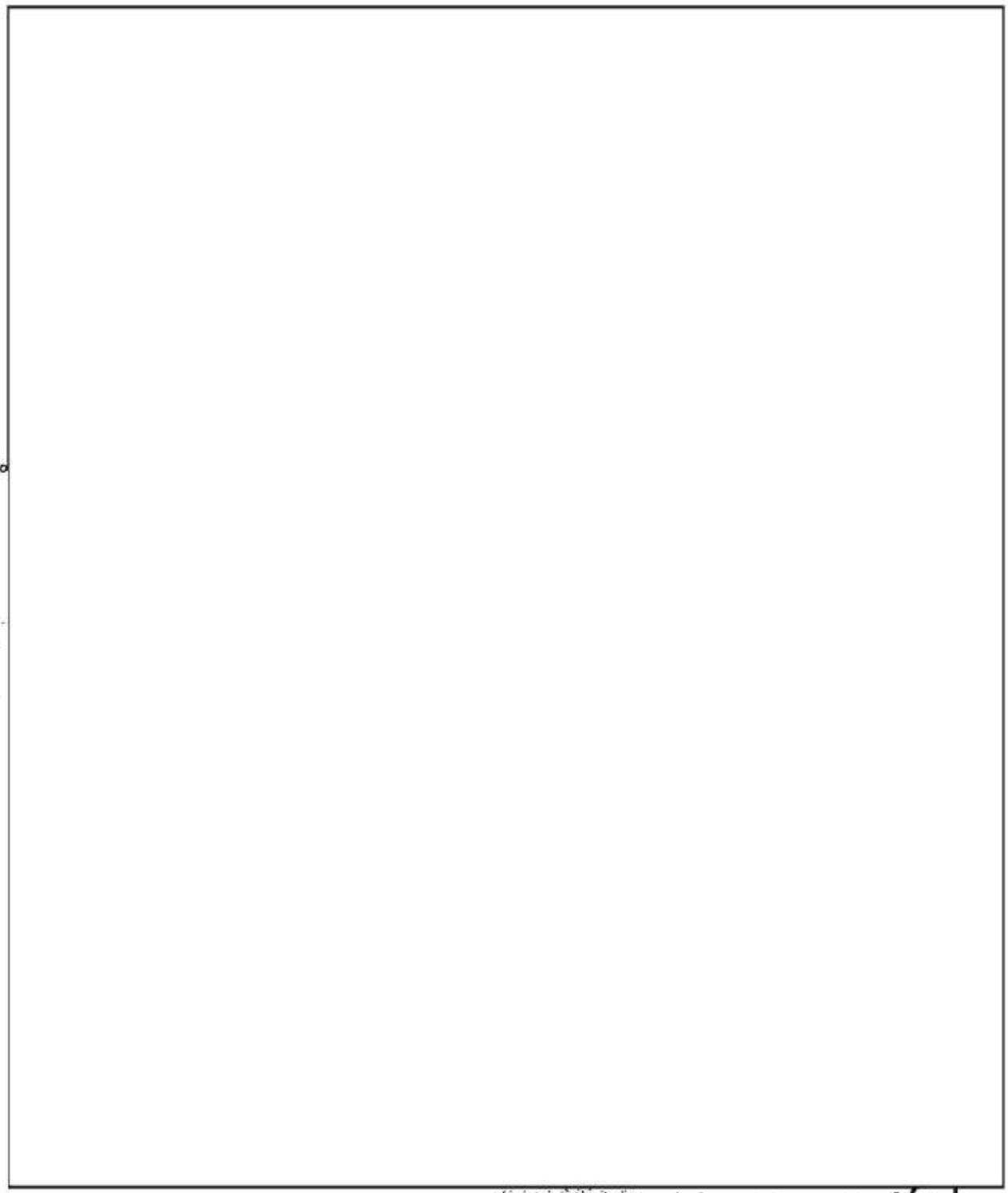
~~TOP SECRET~~ -

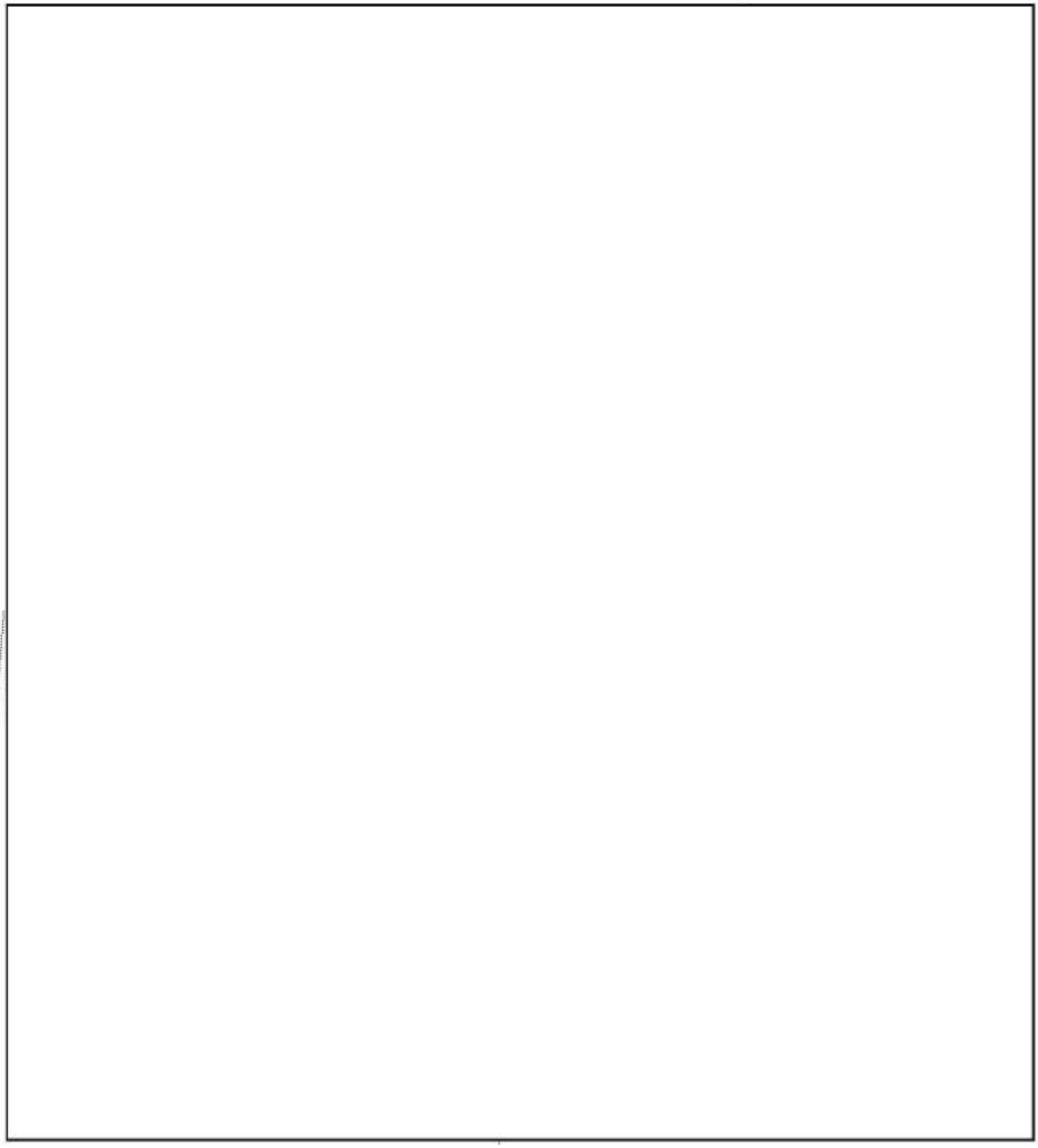
APPENDIX H
Annexure H1 - sheet 5

OGA
EO 1.4.(c)
EO 1.4.(d)

TOP SECRET CONTROL NUMBER 53-7(N)
COPY 100 OF 114 COPIES
PAGE 8 OF 13 PAGES

6.





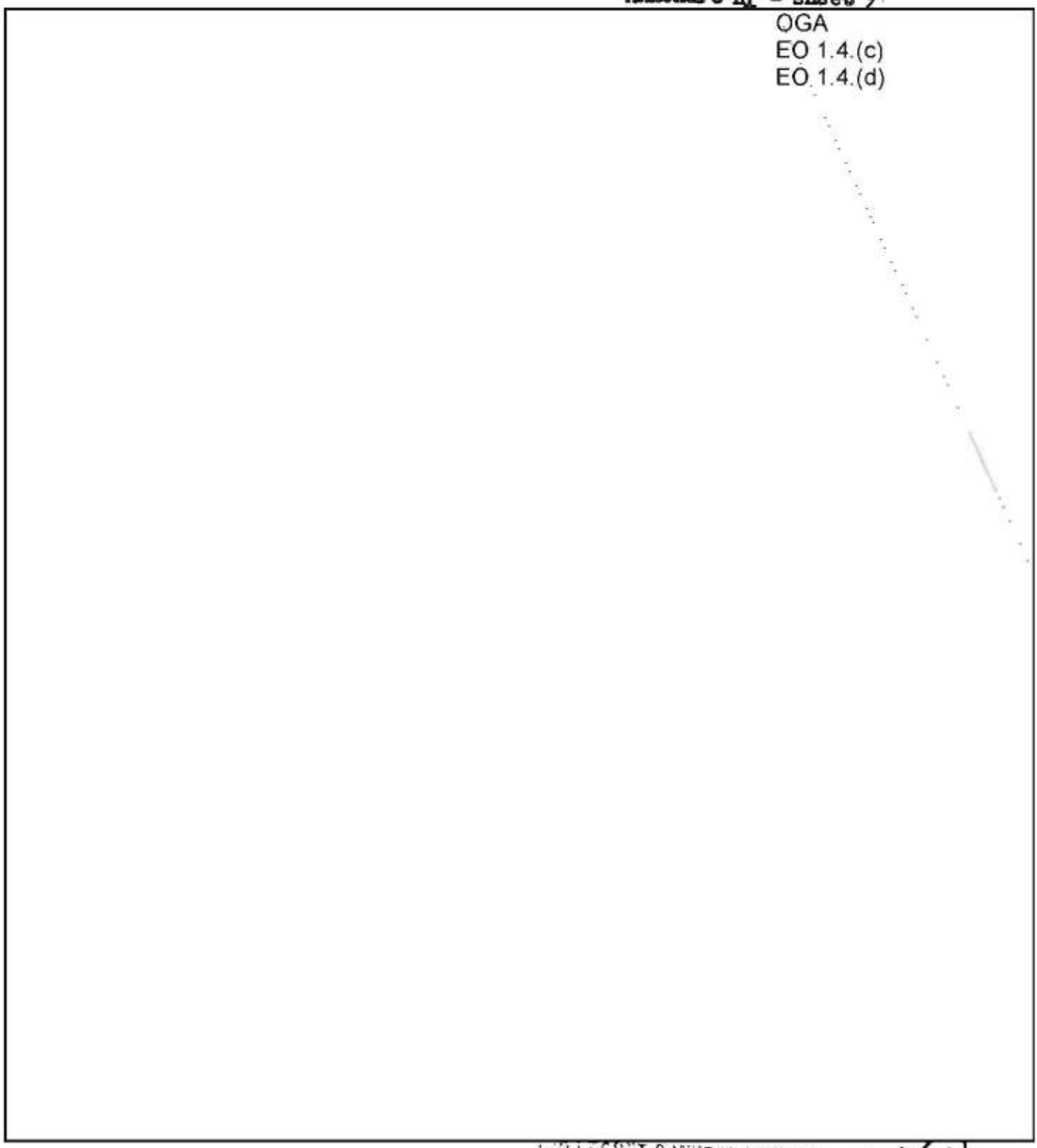
OGA
EO 1.4.(c)
EO 1.4.(d)

TOP SECRET CONTROL NUMBER 53-7(W)-
COPY 100 OF 114 COPIES
PAGE 11 OF 15 PAGES

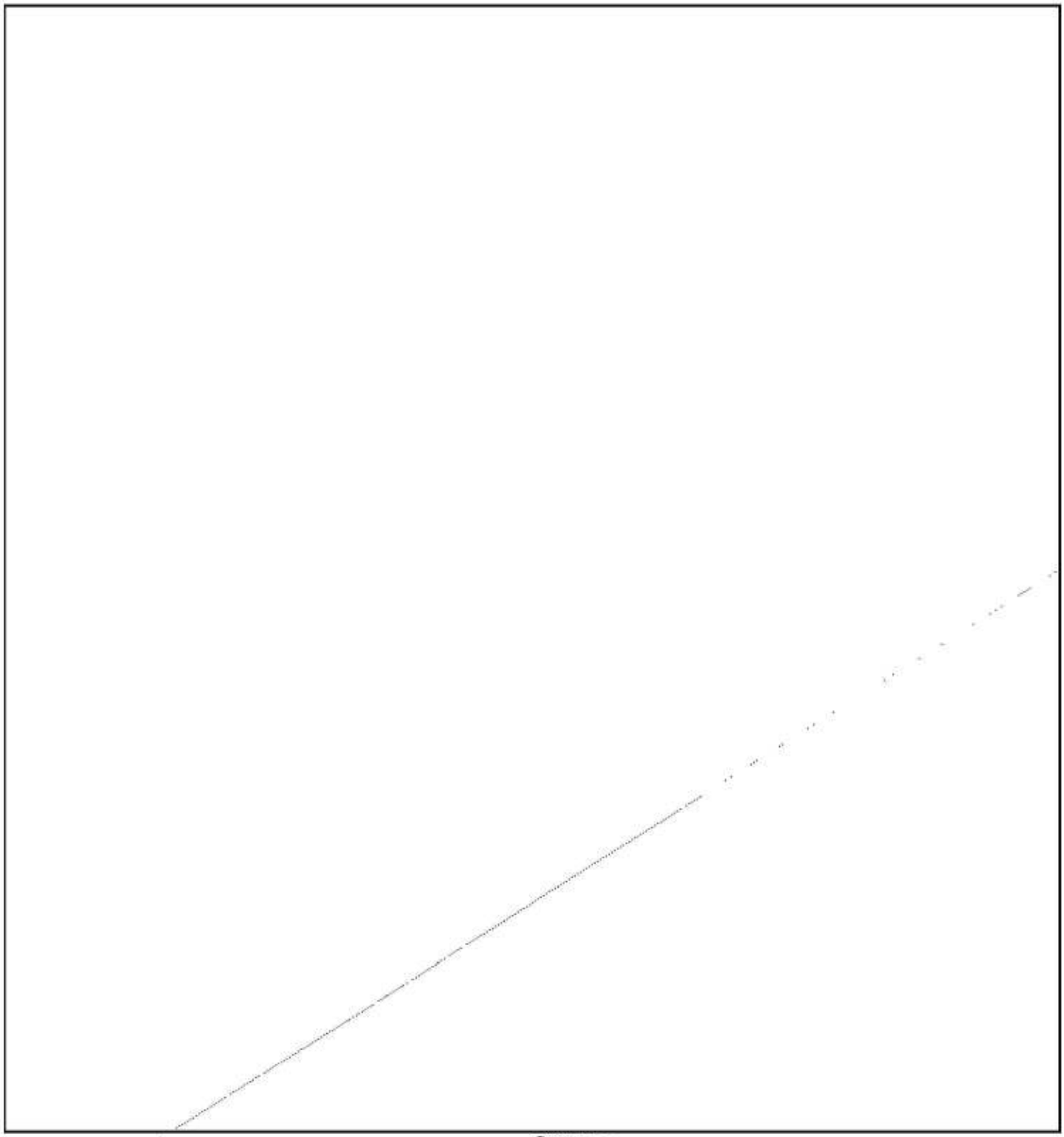
TOP SECRET

APPENDIX H
Annexure H1 - sheet 9

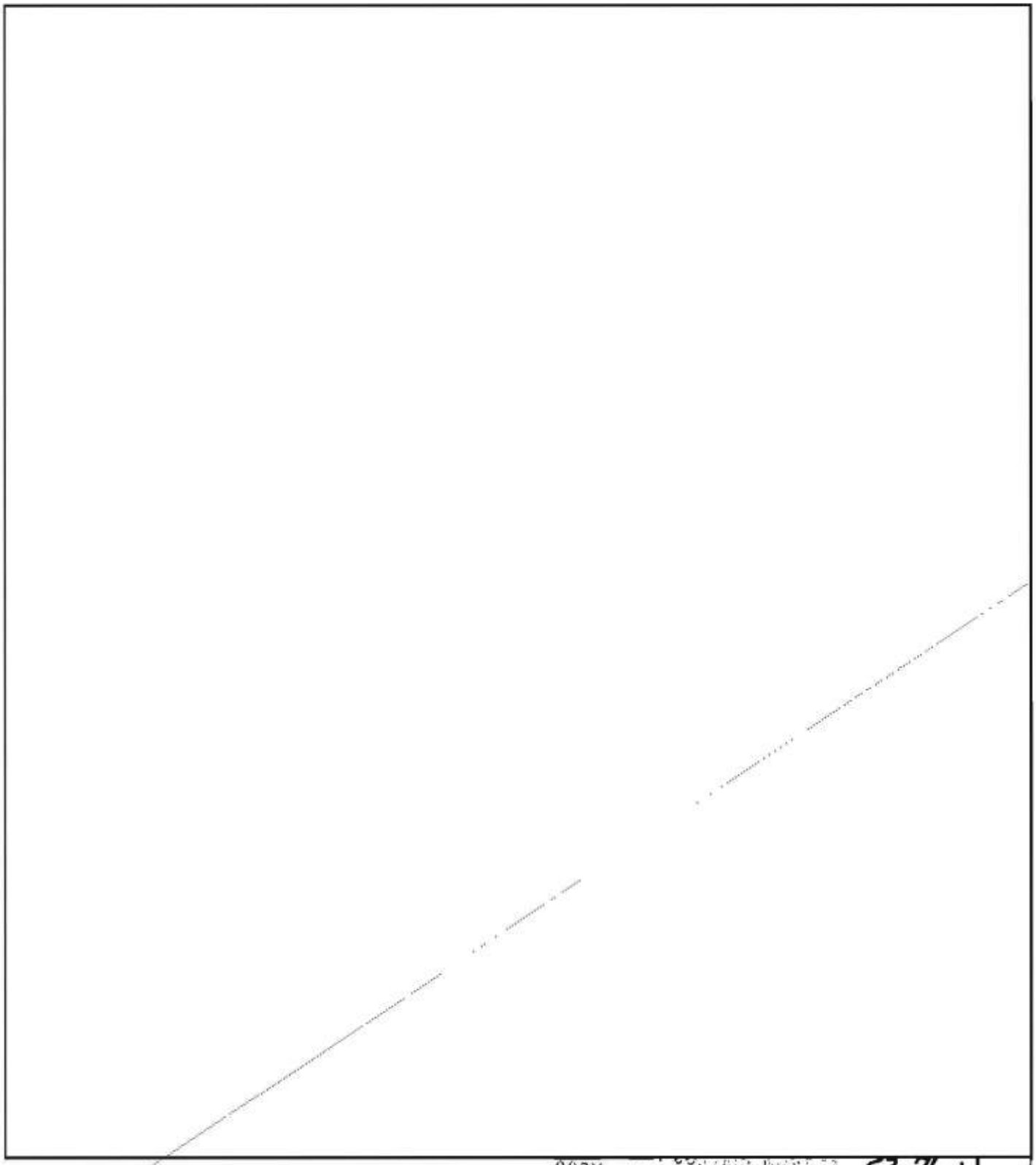
OGA
EO 1.4.(c)
EO 1.4.(d)



TOP SECRET CONTROL NUMBER 53-7(J)
100/12 114/15



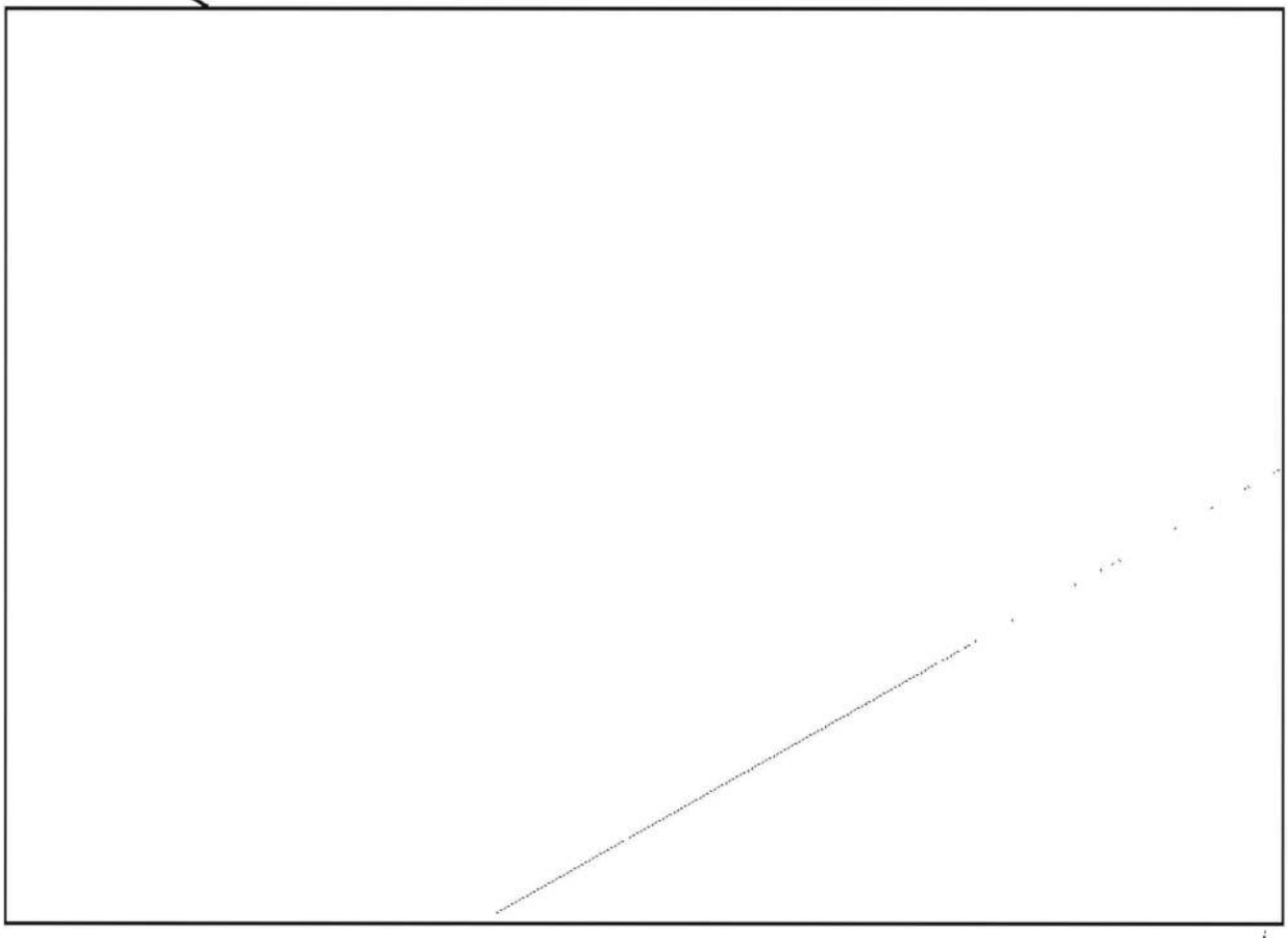
OGA
EO 1.4.(c)
EO 1.4.(d)



OGA
EO 1.4.(c)
EO 1.4.(d)

~~TOP SECRET~~

APPENDIX H
Annexure H_1 - sheet 13



OGA
EO 1.4.(c)
EO 1.4.(d)

TOP SECRET CONTROL NUMBER 53-7(a)+
COPY 100 OF 114 COPIES
PAGE 15 OF 15 PAGES

APPENDIX J

PRINCIPLES OF UKUSA COLLABORATION WITH COMMONWEALTH COUNTRIES OTHER THAN THE U.K.

INTRODUCTION

1. This Appendix records the general principles governing UKUSA Comint collaboration with Commonwealth countries (other than the U.K.) and certain agreements that have been made on Comint policy affecting those countries. For convenience and clarity, certain of the provisions of the U.K.-U.S. Communication Intelligence Agreement, 1946, are incorporated (in paragraphs 2 to 6 below).

GENERAL

2. While Commonwealth countries other than the U.K. are not parties to the U.K.-U.S. Comint agreement, they will not be regarded as Third Parties.

3. L.S.I.B. will, however, keep U.S.C.I.B. informed of any arrangements or proposed arrangements with other Commonwealth agencies.

4. U.S.C.I.B. will make no arrangements with any Commonwealth agency, other than Canadian, except through or with the prior approval of L.S.I.B.

5. As regards Canada, U.S.C.I.B. will complete no arrangements with any agency therein without first obtaining the views of L.S.I.B.

6. It will be conditional on any Commonwealth agencies with whom collaboration takes place that they abide by the terms of paras. 5, 8 and 9 of the U.K.-U.S. Comint agreement and by the arrangements laid down in para. 7 thereof.

ARRANGEMENTS WITH UKUSA-COLLABORATING COMMONWEALTH COUNTRIES

7. At this time only Canada, Australia and New Zealand will be regarded as UKUSA-collaborating Commonwealth countries. In interpretation of para. 3 above L.S.I.B. will not initiate or pursue Comint arrangements with Commonwealth countries other than Canada, Australia and New Zealand (with each of which the L.S.I.B. already has such arrangements) without first obtaining the views of U.S.C.I.B.

8. It is noted that L.S.I.B. has obtained from the Comint authorities of Canada, Australia and New Zealand formal assurances that they will abide by the terms of paras. 5, 8 and 9 of the U.K.-U.S. Comint Agreement and of para. 7 of Appendix E thereto. It is also noted that a prerequisite of Comint collaboration by the U.K. with Canada, Australia and New Zealand was an unequivocal acceptance by those countries of the provisions of the "Explanatory Instructions and Regulations concerning the handling of Signal Intelligence (IRSIG)" by countries, and that continued U.K. Comint collaboration with those countries is dependent on their adherence to the provisions of those regulations.

* That such acceptance has been given by the Comint authorities of those - - - - etc 19....

9. U.S.C.I.B. and L.S.I.B. agree:

(a) not to pass to a collaborating Commonwealth country Comint 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 agencies 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 agencies shall be determined by the Director G.C.H.Q. or the Director N.S.A.; relevant materials shall then be releasable subject to whatever restrictions may be specified by the agency which produced the material (i.e. G.C.H.Q. or N.S.A.).

UKUSA ARRANGEMENTS AFFECTING AUSTRALIA AND NEW ZEALAND

Agreed arrangements affecting Australia and New Zealand are contained in Annexure J1 hereto.

APPENDIX J

ANNEXURE J1

UKUSA ARRANGEMENTS AFFECTING AUSTRALIA AND NEW ZEALAND

1. It is noted that Defence Signals Branch Melbourne (D.S.B.) is, in contrast to Communications Branch Ottawa, not a purely national centre. It is and will continue to be a joint U.K. - 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 L.S.I.B. on the other. On technical matters only, control is exercised by Government Communications Headquarters on behalf of L.S.I.B.

2. G.C.H.Q. will keep N.S.A. informed of the tasks that have been agreed for D.S.B. and will notify N.S.A. in advance before any new or altered task is agreed for D.S.B.

3. N.S.A. and D.S.B. will collaborate directly on those D.S.B. tasks which, as determined by N.S.A., fall within the field of collaboration and will exchange raw material, technical material and end product of these tasks. In addition N.S.A. will provide D.S.B. with raw material technical material and end product as appropriate on other tasks determined by N.S.A. to be relevant to the tasks of D.S.B. A list of tasks under both these heads will be maintained currently by N.S.A. and G.C.H.Q. OGA EO 1.4.(c) EO 1.4.(d)

4. N.S.A. and D.S.B. will also exchange technical interception data relating to the General Search effort of each in the [redacted]

5. Exchanges between N.S.A. and D.S.B. 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 N.S.A. and D.S.B. 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, N.S.A. has accredited liaison officers to D.S.B. and that D.S.B. will accredit a liaison officer or officers to N.S.A. when it is in a position to do so.

8. It is further noted that, in interpretation of Appendix I to the UKUSA agreement, U.S.C.I.B. will possibly decide at some future date to modify the terms of reference for the senior liaison officer now accredited to D.S.B., whereby he will be the senior U.S. representative for conduction liaison with Australia and New Zealand and, as may be agreed by L.S.I.B., with U.K. officials in those countries, on matters pertaining to Comint.

BPC 53/N/Final
041

OGA
EO 1.4.(c)
EO 1.4.(d)

19 March 1953

Appendix (N)

ARRANGEMENTS FOR EMERGENCY RE-LOCATION OF COMINT UNITS

[redacted]

BPC 53/N/Final
041
19 March 1953

OGA
EO 1.4.(c)
EO 1.4.(d)

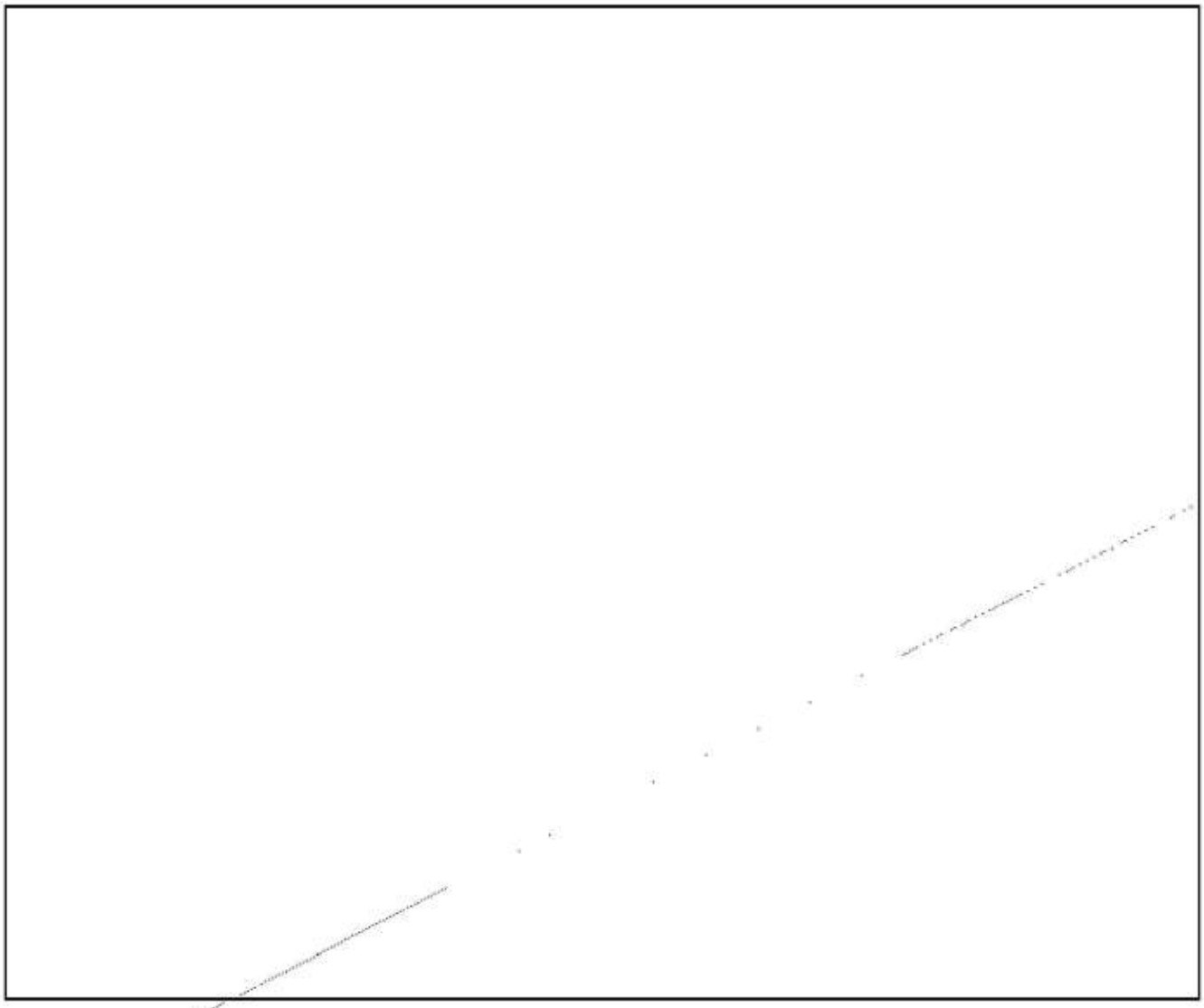
~~TOP SECRET CANOE - SECURITY INFORMATION~~

BPC 53/N/Final
041
19 March 1953
Appendix (N)

OGA
EO 1.4.(c)
EO 1.4.(d)

OGA
EO 1.4.(c)
EO 1.4.(d)

BPC 53/N/ Final
041
19 March 1953
Appendix (N)



OGA
EO 1.4.(c)
EO 1.4.(d)

BPC 53/N/Final
041

OGA
EO 1.4.(c)
EO 1.4.(d)

19 March 1953

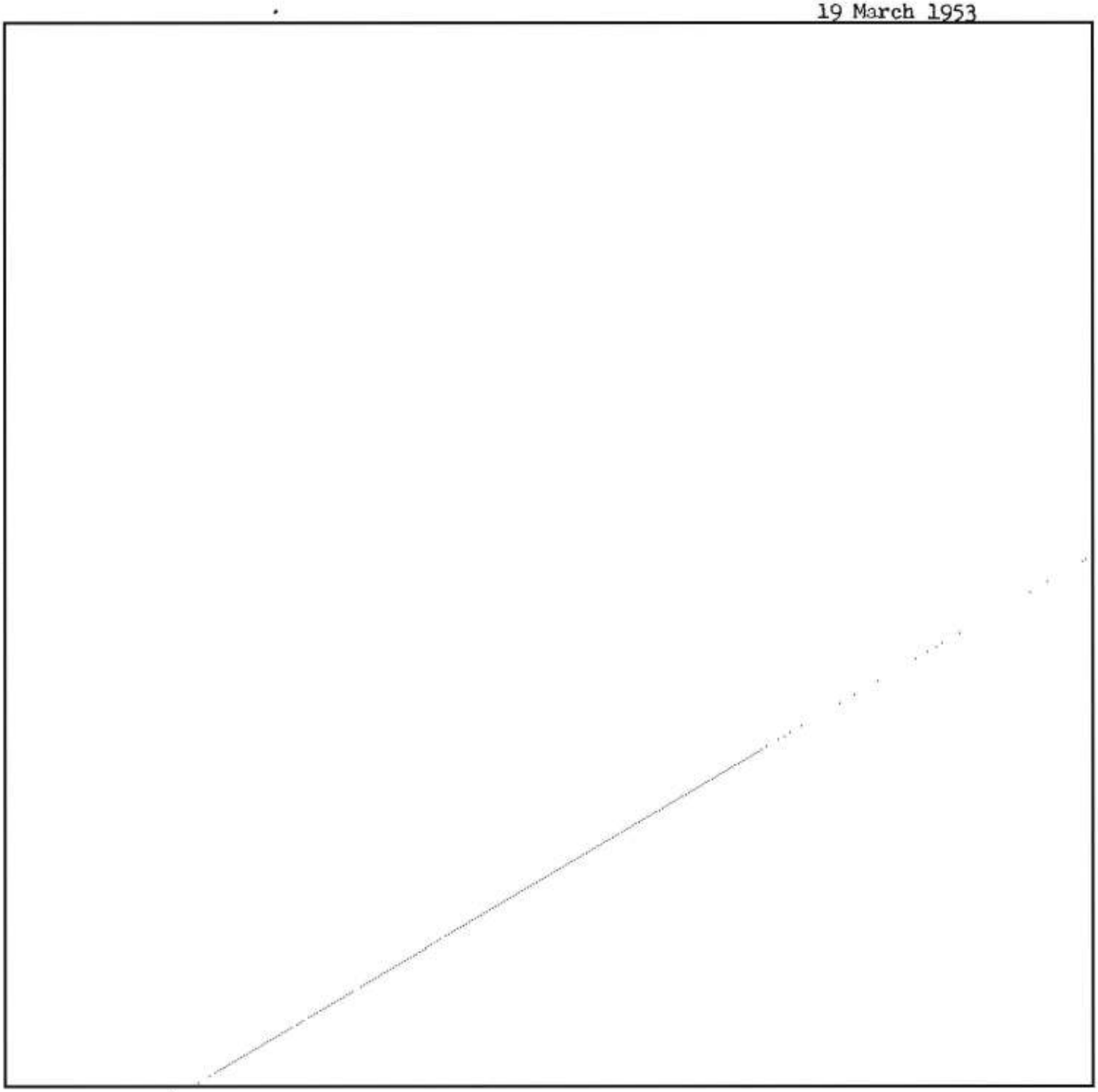
APPENDIX 'N'

ANNEXURE N1

RE-LOCATION OF U.S. AND U.K. COMINT UNITS

OGA
EO 1.4.(c)
EO 1.4.(d)

BPC 53/N/Final
041
19 March 1953



OGA
EO 1.4.(c)
EO 1.4.(d)

BPC53/N/Final
041
19 March 1953

APPENDIX 'N'
ANNEXURE N2

OGA
EO 1.4.(c)
EO 1.4.(d)

~~RESTRICTED~~

EPC53/N/Final
041
19 March 1953

~~RESTRICTED - SECURITY INFORMATION~~

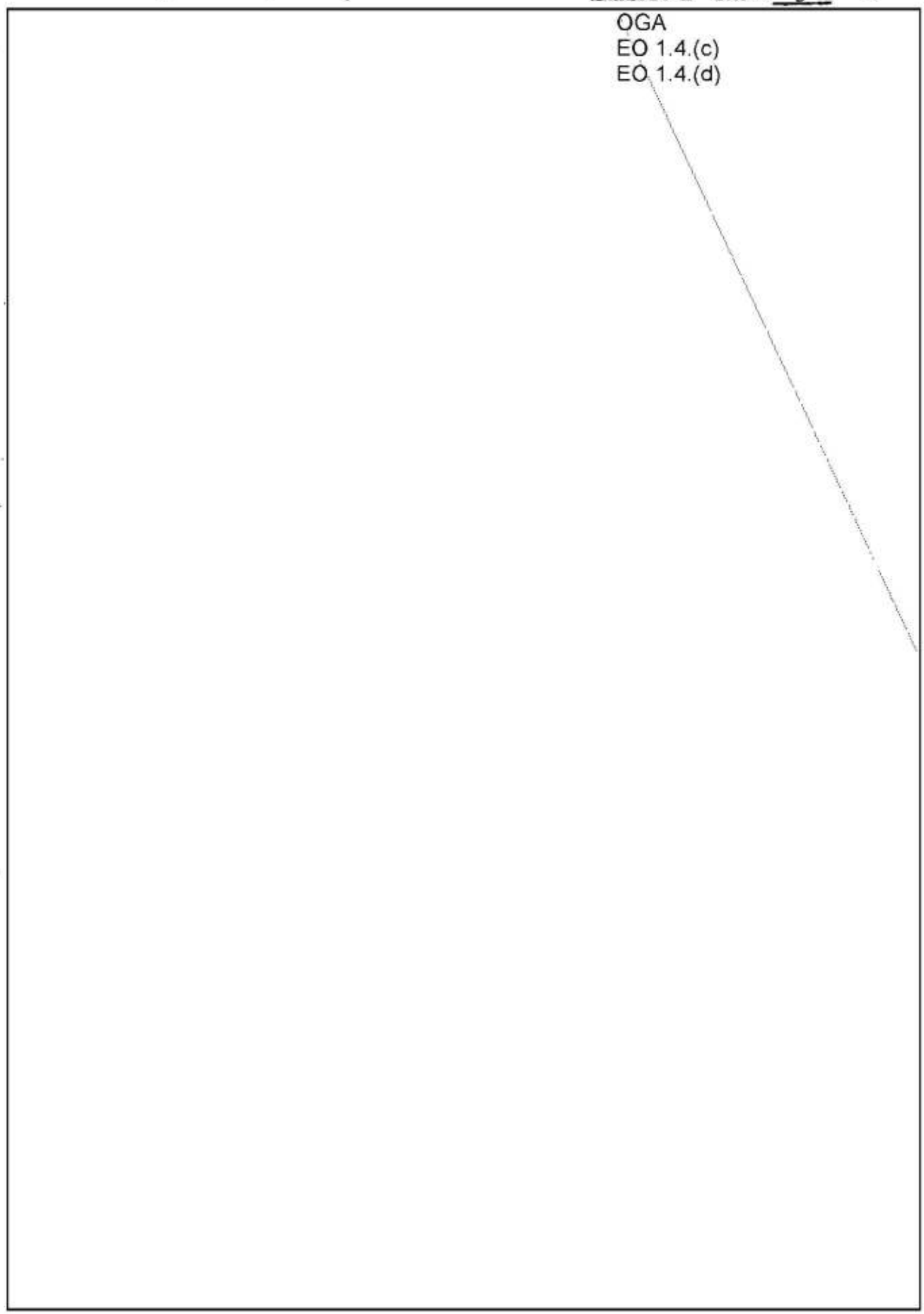
Exhibit I Sheet 1

APPENDIX N
Annexure N1
Exhibit 1

OGA
EO 1.4.(c)
EO 1.4.(d)

~~[RESTRICTED SECURITY INFORMATION]~~

OGA
EO 1.4.(c)
EO 1.4.(d)


OGA
EO 1.4.(c)
EO 1.4.(d)

OGA
EO 1.4.(c)
EO 1.4.(d)

OGA
EO 1.4.(c)
EO 1.4.(d)

EFC 53/0 FINAL
042

19 March 1953

REVIEW OF APPENDIX O WITH REFERENCE TO

OGA
EO 1.4.(c)
EO 1.4.(d)

OGA
EO 1.4.(c)
EO 1.4.(d)

OGA
EO 1.4.(c)
EO 1.4.(d)

19 March 1953

[redacted]

OGA
EO 1.4.(c)
EO 1.4.(d)

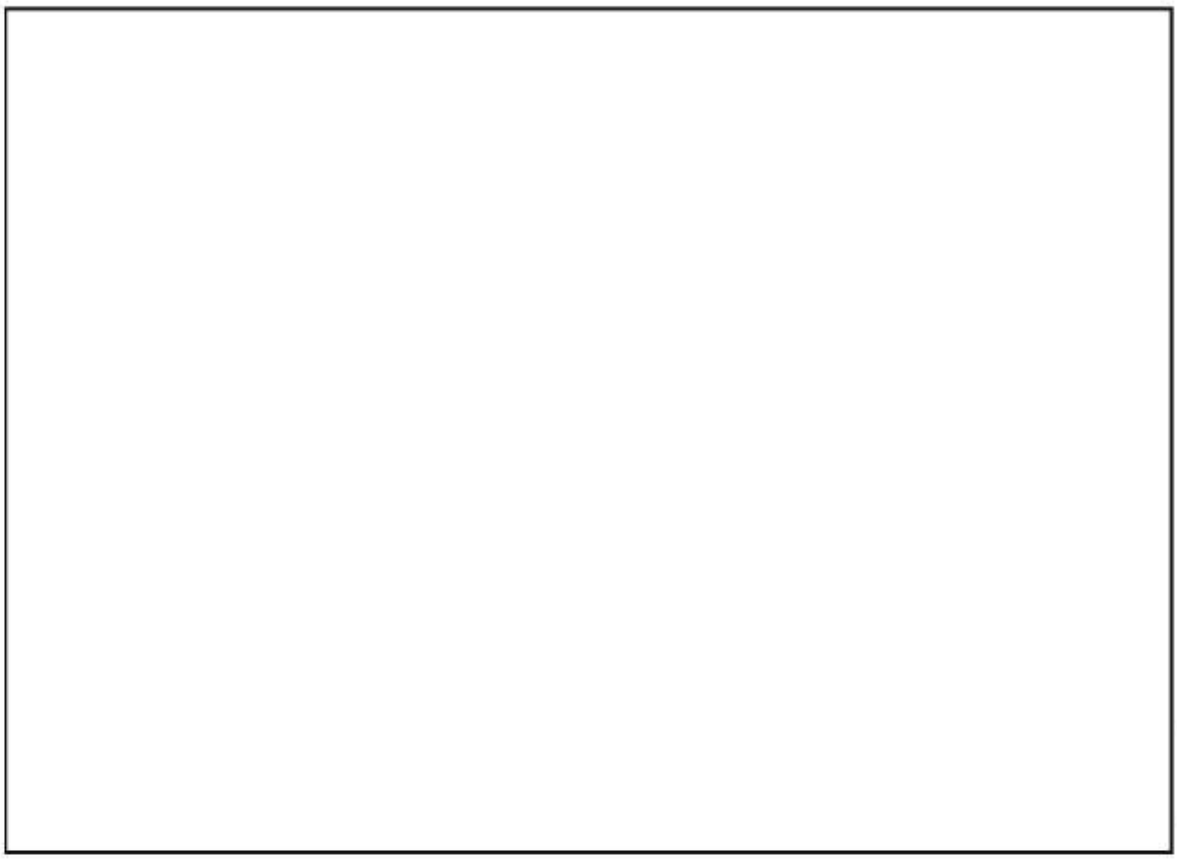
BPC53/0 FINAL
042

19 March 1953

OGA
EO 1.4.(c)
EO 1.4.(d)

19 March 1953

OGA
EO 1.4.(c)
EO 1.4.(d)



OGA
EO 1.4.(c)
EO 1.4.(d)

LAWFARE

SECRECY: FOIA

Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements

By **Scarlet Kim**, **Diana Lee**, **Asaf Lubin**, **Paulina Perlin** Monday, April 23, 2018, 5:00 PM

The United States is party to a number of international intelligence sharing arrangements—one of the most prominent being the so-called "Five Eyes" alliance. Born from spying arrangements forged during World War II, the Five Eyes alliance facilitates the sharing of signals intelligence among the U.S., the U.K., Australia, Canada and New Zealand. The Five Eyes countries agree to exchange by default all signals intelligence they gather, as well as methods and techniques related to signals intelligence operations. When the Five Eyes first agreed to this exchange of intelligence—before the first transatlantic telephone cable was laid—they could hardly have anticipated the technological advances that awaited them. Yet, we remain in the dark about the current legal framework governing intelligence sharing among the Five Eyes, including the types of information that the U.S. government accesses and the rules that govern U.S. intelligence agencies' access to and dissemination of Americans' private communications and data.

In July 2017, Privacy International and Yale Law School's Media Freedom & Information Access Clinic filed a lawsuit against the National Security Agency, the Office of the Director of National Intelligence, the State Department, and the National Archives and Records Administration seeking access to records related to the Five Eyes alliance under the Freedom of Information Act. Over the past few months, we have begun to receive limited disclosure from the NSA and the State Department. While we have not seen the text of the current agreement—as well as other records that would shed important light on how the agreement operates—the disclosures to date give us insight into the nature and scope of U.S. intelligence sharing agreements.

Below, we summarize a few of these disclosures and talk through their implications. In particular, we highlight how, taken together, they suggest that the U.S. government takes an inconsistent approach to legal classification and therefore publication of these types of agreements. We also take a closer look at one agreement—the 1961 General Security Agreement between the Government of the United States and the Government of the United Kingdom—which further illuminates our understanding of the privatization of intelligence activities and provides us with a rare glimpse of the "third party rule," an obstacle to oversight and accountability of intelligence sharing.

The Disclosures

1959-61 Appendices to the United Kingdom-United States Communication Intelligence (UKUSA) Agreement

The sharing arrangements undergirding the Five Eyes alliance were first memorialized in the British-U.S. Communication Intelligence Agreement in 1946, later renamed the United Kingdom-United States Communication Intelligence Agreement. At the time we brought our lawsuit, the 1956 version of the that agreement was the most recent publicly available. In response to our litigation, the NSA disclosed several appendices that span from 1956–61 and therefore update our understanding of the agreement by several years.

1961 General Security Agreement between the Government of the United States and the Government of the United Kingdom (General Security Agreement)

The State Department disclosed the General Security Agreement as well as a set of procedures developed to implement the provisions of that agreement. The General Security Agreement relates to the protection of classified information exchanged between the U.S. and the U.K. and provides that "[o]fficial information given a security classification by either of [the] two Governments … and furnished by either Government to the other through Government channels will be assigned a classification by … the receiving Government which will assure a degree of protection equivalent to or greater than that

required by the Government furnishing the information." The State Department also disclosed an exchange of letters between then-U.K. Ambassador to the U.S. Harold Caccia and then-U.S. Secretary of State Dean Rusk expressing their respective governments' acceptance of the terms of the agreement.

1998 Agreement to Extend the 1966 Agreement between the Government of Australia and the Government of the United States of America relating to the Establishment of a Joint Defence Facility at Pine Gap (Pine Gap Agreement)

The State Department disclosed an exchange of letters between then-Australian Minister for Foreign Affairs Alexander Downer and then-U.S. Ambassador to Australia Genta Holmes expressing their respective governments' agreement to extend the terms of the 1966 "Agreement between the Government of Australia and the Government of the United States of America relating to the Establishment of a Joint Defence Facility at Pine Gap." Pine Gap is a base located in Alice Springs, Australia jointly operated by the U.S. and Australia. From Pine Gap, the U.S. controls satellites across several continents, which can conduct surveillance of wireless communications, such as those transmitted via cell phones, radios and satellite uplinks. The intelligence gathered supports both intelligence activities and military operations, including drone strikes.

The letters express the U.S. and Australian governments' agreement to extend the Pine Gap Agreement "for a period of ten years from 16 November 1998" and to have it remain in force thereafter "until terminated." The letter from Downer to Holmes expressly proposes that

---

this Note and your confirmatory reply thereto shall together constitute an Agreement between our two Governments concerning this matter which shall enter into force on the date that the Government of Australia notifies the Government of the United States of America that all domestic procedures as are necessary to give effect to this Agreement in Australia have been satisfied.

Observations

An Inconsistent Approach to International Agreements

The Pine Gap and General Security Agreements described above differ in a notable respect: While the 1998 extension to the Pine Gap Agreement is available to the U.S. public, the 1961 General Security Agreement has not been published by the United States. This difference reveals gaps in the laws requiring the publication of international agreements. And it bolsters calls, raised elsewhere, for greater executive branch transparency and accountability in the formation and legal bases of these types of agreements.

The United States plainly considers the 1998 extension to the Pine Gap Agreement a legally binding international agreement. The U.S. State Department has made the 1998 Pine Gap Agreement publicly available in the Treaties and Other International Agreements Series (TIAS), a repository which serves as "competent evidence" of the treaties and other international agreements entered into by the United States. 1 U.S.C. § 113. Likewise, the Australian government has published the Pine Gap Agreement in the Australian Treaty Series. But whereas the Australian government has also published the text of the *original* 1966 Pine Gap Agreement, the United States has not. This omission is significant. Only the 1966 agreement contains the terms agreed upon by both parties—in other words, the nature and scope of the agreement to establish a joint defense facility to conduct intelligence activities.

Similarly, neither the U.S. nor the U.K. appear to have published the 1961 General Security Agreement. According to the U.K. government's response to a Parliamentary question in 2000, the General Security Agreement had not been declassified at that time. Searching through a variety of publicly available materials, including government websites and academic databases, we found several references to the General Security Agreement, but not the Agreement itself (nor portions of it). For example, the 2007 Treaty with United Kingdom Concerning Defense Trade Cooperation recognizes "principles established under the General Security Agreement." However, prior to the State Department's disclosure in response to our FOIA request, we did not know what these principles were.

There is a colorable argument that State has a legal duty to publish both the original text of the Pine Gap Agreement and the 1966 General Security Agreement, as well as any updates to both. Under 1 U.S.C. § 112a, the Secretary of State is required to publish all treaties and non-treaty international agreements to which the United States is a party. This duty is subject to a short list of exceptions outlined in § 112a(b). Most notably, the State Department may elect not to publish an international agreement if, "in the opinion of the President," disclosure would prejudice national security interests.

The government could justify its failure to publish the agreements on two grounds. First, the national security exemption might apply. However, this claim falls apart in light of the facts that the original Pine Gap Agreement has already been published by the Australian government and the United Nations, and State released the General Security Agreement in response to a FOIA request notwithstanding FOIA's national security exemption in 5 U.S.C. § 552(b)(1).

A second argument could be made that at the time of their formation, the U.S. State Department did not consider the 1966 Pine Gap Agreement and the General Security Agreement to be binding international agreements. Under current U.S. law, legally binding international agreements may take the form of treaties or executive agreements. The majority of U.S. international agreements are executive agreements, which, as the Congressional Research Service outlines, take three general forms:

---

(1) congressional-executive agreements, in which Congress has previously or retroactively authorized an international agreement entered into by the Executive;

(2) executive agreements made pursuant to an earlier treaty, in which the agreement is authorized by a ratified treaty; and

(3) sole executive agreements, in which an agreement is made pursuant to the President's constitutional authority without further congressional authorization.

The 1966 Pine Gap Agreement and the General Security Agreement appear to fall into the third category. Both were formed under the executive's Article II powers in foreign affairs and national security and without congressional authorization.

Prior to the 1970s, executive agreements were unregulated and undefined. Indeed, it was not until after the Case-Zablocki Act's passage in 1971 that the State Department outlined criteria for identifying non-treaty international agreements. By this logic, the United States perhaps did not publish the agreements because it did not understand them to trigger § 112a's publication requirement at the time they were signed.

This argument, however, is suspect because both agreements appear to remain in force. In fact, evidence suggests that the 1966 General Security Agreement is not the most recent version in effect. The British House of Commons referenced 1983 and 1984 amendments to the General Security Agreement, as well as a "new Security Implementing Arrangement for operations between the [U.K. Ministry of Defense] and the [U.S. Department of Defense]" formed in 2003. And since it was the State Department that gave us these disclosures, State possessed these agreements (and even recognized the Pine Gap Agreement in the TIAS). Accordingly, the State Department should have published the agreements pursuant to § 112a.

The U.S. government's failure to publish these agreement adds to longstanding confusion about what constitutes an international agreement under U.S. law, their legal bases, how many have been formed, and what they contain. It also makes it more difficult for the public to hold the government accountable. As others have noted, "Today nearly all of U.S. international law is made by the President acting alone with little oversight by Congress or the U.S. public." Put simply, members of the public should not have to undertake lengthy FOIA processes (these disclosures were made nearly a year after we filed our request) in order to uncover the text of agreements that underpin our understandings of national security and international cooperation.

The 1961 General Security Agreement

Below, we take a closer look at the 1961 General Security Agreement. In particular, we consider its provisions on the role of private contractors, which contributes to our understanding of the privatization of intelligence activities. We further consider the General Security Agreement's invocation of the "third party rule," a rarely-seen but common feature of intelligence sharing agreements, which presents a challenge to the effective oversight and accountability of intelligence sharing.

The History of Privatizing Espionage

The 1961 General Security Agreement sheds important light on the history and scope of the privatization of espionage, particularly during the formative years of the U.S. intelligence community. A substantive body of literature on this topic does exist, one prime example being Tim Shorrock's "Spies for Hire," which discusses the "American Intelligence-Industrial Complex, the agencies it serves, its key industrial players, and the former high-ranking national security officials who run its largest companies." In his book, Shorrock maps out the historical origins and underpinnings of this partnership. For instance, he describes how the CIA contracted with Lockheed Corporation to build the U-2 Spy planes, which were used to gather intelligence during the Cold War, including on the Soviet Union and the People's Republic of China. He also describes how the CIA contracted with General Electric, Itek, and Lockheed to commission the CORONA photoreconnaissance satellites, which catalogued Soviet ICBM complexes. The CIA was hardly the only government player in such partnerships. As Shorrock highlights, "outsourcing has always been part of the U.S. spying enterprise," suggesting that other parts of the U.S. intelligence community have long been involved in the practice. For example, in the 1950s, IBM, Bell Labs, and Cray developed the first supercomputers and encryption equipment which the NSA "used to crack coded diplomatic and military messages and convert huge volumes of signals intelligence into actionable intelligence."

Much of the existing literature focuses on the relationship between the U.S. intelligence community and American corporations, but very little is known about outsourcing from U.S. intelligence agencies to foreign corporations and from foreign intelligence agencies to U.S. corporations. Even less is known about the level of access that foreign contractors might have to classified American intelligence. The "Industrial Security Annex" of the General Security Agreement sheds some light on these relationships:

The Annex governs "those cases in which contracts, subcontracts, precontract negotiations or other government approved arrangements involving classified information of either or both countries, hereinafter referred to as classified contracts, are placed or entered into by or on behalf of the" U.K. or U.S. governments.

The Annex provides a mechanism by which U.S or U.K. contractors can be treated as government entities for the purposes of sharing classified information. The general rule is that "[t]ransmission of classified information and material shall be made only through representatives designated by each of the governments … known as transmission through government-to-government channels." But

---

[a]s an exception, the US may transmit classified material directly to a firm located in the US which is under the ownership, control, or influence of a UK entity, and the UK may transmit such information directly to a firm in the UK which is under the ownership, control, or influence of a US entity provided such firms have been granted a reciprocal security clearance … and the information is determined to be releasable under the national disclosure policy of the releasing government.

In very limited circumstances, the Annex also provides a mechanism by which non-U.S/U.K. contractors might be "eligible to be awarded classified contracts." The general rule is that "[f]irms which are under the ownership, control, or influence of a third party country are not eligible." But "[r]equests for exception to this requirement may be considered on a case-by-case basis by the releasing government."

As Shorrock notes "many of the companies that dominate the intelligence industry today got their start by providing technical services and products to the Intelligence Community." The conventional wisdom is thus that the public-private partnerships of the 1950s and 1960s were predominantly of a technological nature, namely to facilitate the development of new surveillance capabilities. One would therefore expect the Industrial Security Annex to limit the scope of access by

contractors to information strictly necessary to accomplish those kinds of technical assignments. In reality, however, the Annex places no such limitation on the type of information that may be shared with contractors. Rather, the Annex covers the transmission of "classified information in any form, be it oral, visual or in the form of material," and defines material as encompassing "everything regardless of its physical character or makeup including" documents, writing, maps and letters. Furthermore, the Annex establishes no criteria for what intelligence community activities may be outsourced, whether they may be outsourced to foreign contractors, and under what circumstances.

Scholars have, in the past, raised concerns about the privatization of espionage. For example, Professor Martin Trybus has argued that privatizing intelligence work degrades a set of fundamental objectives:

First, democracy and the rule of law are compromised. Escaping parliamentary and judicial scrutiny are important reasons for privatisation in the first place. Second, value for money is compromised since the private sector operates at higher costs and the necessity of security clearances limits competition to an extent undermining the economic rationale for privatisation in this sector dominated by national security and secrecy concerns. Finally, national security is compromised by the higher costs for intelligence on the one hand and intelligence and know-how being transferred outside the intelligence agencies on the other hand. The public interest enshrined in the three objectives of the triangle does not appear to be served by the current state of privatisation of intelligence services in the United States.

The privatization of espionage also raises concerns about the outsourcing of inherently governmental functions. U.S. law has long prohibited contractors from performing such functions. But there is insufficient guidance on what constitutes "inherently governmental functions." (For a review of conflicting definitions under U.S. law, see this 2009 summary by the Congressional Research Service). For example, should a private contractor be permitted to engage in target selection or intelligence analysis and verification? Professor Simon Chesterman has noted that "uncertainty in this area appears to be intentional and thus exacerbates the accountability challenges posed by secrecy and problematic incentives."

The "Third Party Rule" or the "Originator Control Principle"

The 1961 General Security Agreement also provides a rare glimpse of the "third party rule" or "originator control principle," considered a common feature of many intelligence sharing arrangements. The third party rule prohibits the disclosure of information shared between agencies to third parties, which may include oversight bodies, without the prior consent of the state from which the information originated. As Privacy International has noted, such rules limit oversight and weaken accountability of intelligence sharing.

While the use of the third party rule is commonly remarked upon in discussions of intelligence sharing (by both civil society and multilateral organizations), we have had few opportunities to see what the rule actually looks like in practice, as intelligence sharing agreements are rarely subject to public scrutiny. The General Security Agreement contains two different articulations of the third party rule: one contained within the letter exchange concerning the Agreement from the U.S. to the U.K. and the other within an annex to the Agreement on General Security Procedures. The former is more expressive and less stringent than the latter and reads as follows:

Recognizing that the protection of all classified information communicated directly or indirectly between our governments is essential to the national safety and security of both our countries, I have the honor to suggest the following mutual understanding for the protection of such information, namely, that the recipient:

a. Will not release the information to a third Government without the approval of the releasing Government.

b. Will undertake to afford the information substantially the same degree of protection afforded to it by the releasing Government.

c. Will not use the information for other than the purpose given.

d. Will respect private rights, such as patents, copyrights, or trade secrets which are involved in the information." (emphasis added)

The third party rule as expressed in the Annex is far shorter, stating: "The recipient government will not use such information for other than the purposes for which it was furnished and will not disclose such information to a third Government without the prior consent of the Government which furnished the information."

As articulated, the third party rule illustrates the desire for a partner agency to retain some measure of control over shared information. In some instances, that control might also protect human rights. For example, the rule helps to prevent the further dissemination of shared information to third party agencies, particularly those that the originating agency is concerned would potentially misuse the information. One example of misuse is the Maher Arar case where the Canadian government produced inaccurate intelligence, which was later shared with the U.S. government. The U.S. government subsequently detained Mr. Arar for 12 days and then proceeded to subject him to rendition in Syria where he was tortured.

Governments have also interpreted the third party rule as prohibiting disclosure to other third parties and have included oversight bodies within that prohibition. Under this interpretation, the rule can be fundamentally detrimental to intelligence oversight. As a matter of principle, requiring oversight bodies to seek consent from a foreign agency to access intelligence information shared with a domestic agency can cripple their capacity to exercise independent and impartial oversight. And as a matter of practice, foreign partners are unlikely to consent to such requests. Seeing the two different articulations of the third party rule in the General Security Agreement highlights that there is no "one size fits all" phraseology for the rule. Alternative versions of the rule attentive to human rights might include, for example, a carve-out that would explicitly permit oversight bodies in both countries to review shared information.

Correction: A previous version of this post incorrectly identified the extension to the Pine Gap agreement as agreed to in 1988. The extension agreement was reached in 1998.

Topics: Intelligence Oversight, Secrecy: FOIA

Scarlet Kim was formerly a Legal Officer at Privacy International, a UK-based human rights NGO focused on issues arising at the intersection of privacy and technology. Scarlet also previously worked as an Associate Legal Adviser at the International Criminal Court and as a Gruber Fellow in Global Justice at the New York Civil Liberties Union. She served as a clerk on the U.S. District Court for the Eastern District of New York and is a graduate of Yale Law School. She is a U.S.-qualified lawyer and is admitted as a Solicitor in England and Wales.

Diana Lee is a J.D. candidate at Yale Law School.

Asaf Lubin is an S.J.D. candidate at Yale Law School.

Paulina Perlin is a J.D. candidate at Yale Law School.

Privacy International v. NSA et al. (US 5EY FOIA)

United States District Court for the District of Columbia

Case No. 17-cv-01324

Status: Open

On 5 July 2017, Privacy International filed a Freedom of Information Act ("FOIA") lawsuit seeking to compel the disclosure of records relating to a surveillance agreement governing the exchange of signals intelligence between the governments of the U.S., U.K., Canada, Australia and New Zealand ("Five Eyes alliance"). Privacy International is represented by the Media Freedom Information Access Clinic at Yale Law School.

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 Communications Intelligence Agreement ("UKUSA Agreement"), first signed in 1946. Pursuant to the UKUSA Agreement, the Five Eyes countries agree to exchange by default *all* signals intelligence they gather, as well as the methods and techniques related to signals intelligence operations.

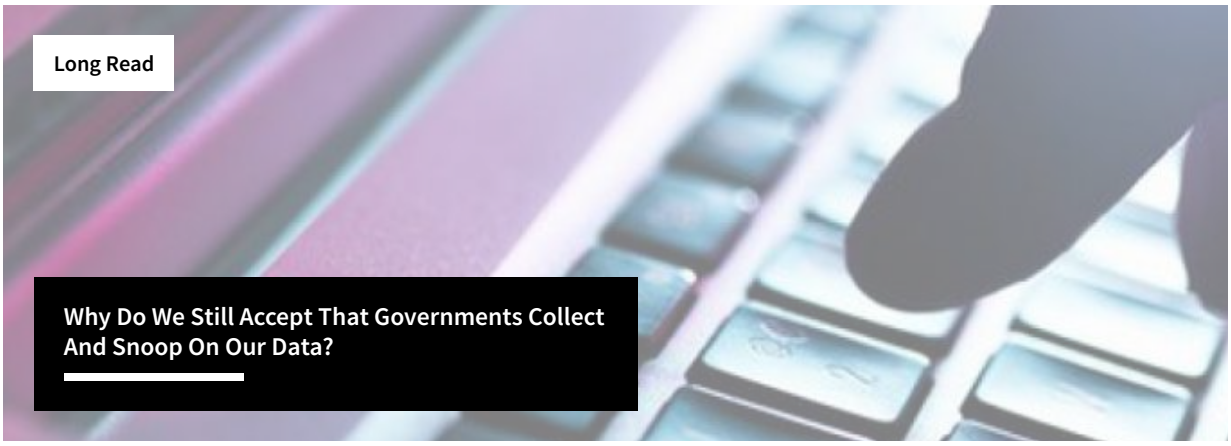
A **1955 version of the Agreement** is the most recent version to have been made public. Communications methods have changed dramatically since 1955, vastly increasing the opportunities for governments to acquire, store and/or analyse communications and data and to share that information with other governments. The nature of signals intelligence has also changed dramatically since 1955. As modern communications have evolved, intelligence agencies have developed more advanced ways to access, acquire, store, analyse and disseminate information.

Privacy International has sought for years to obtain information about the UKUSA Agreement and the rules governing the Five Eyes alliance via freedom of information

requests and other methods. In the U.S., Privacy International has made FOIA requests to the National Security Agency ("NSA"), the Office of the Director of National Intelligence ("ODNI"), the State Department ("State), and the National Archives and Records Administration ("NARA").

Privacy International's requests seek the current text of the UKUSA Agreement and the rules and regulations governing the exchange of signals intelligence pursuant to the Agreement. Privacy International seeks these records so as to determine whether the Five Eyes intelligence sharing activities appropriately accommodate the constitutional rights of American citizens and residents as well as the human rights of non-American citizens and residents.

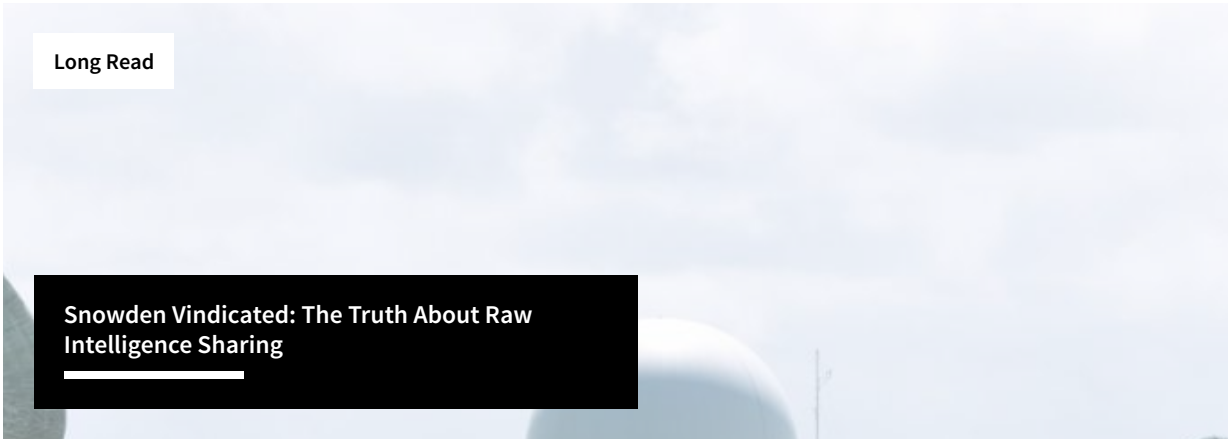
Reports and Analysis



Five Eyes Integration and the Law

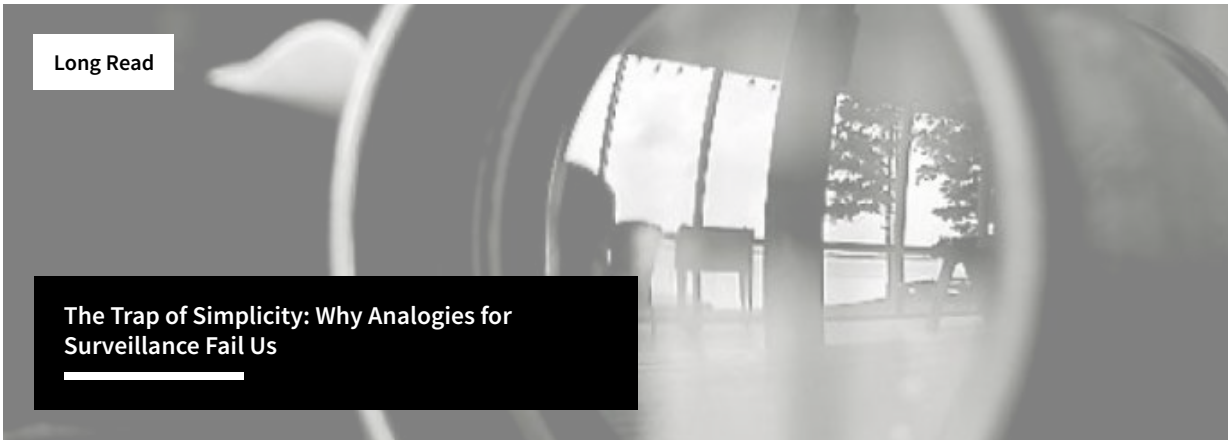
Long Read

The Snoopers' Loophole: Why Winning Against GCHQ Is Bittersweet



Long Read

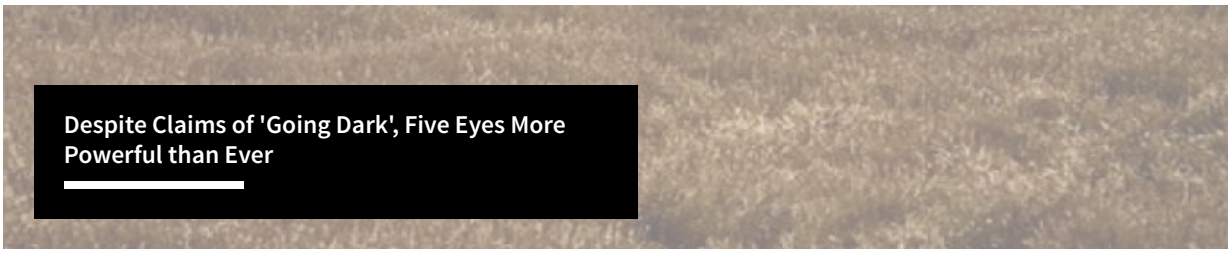
Snowden Vindicated: The Truth About Raw Intelligence Sharing



Long Read

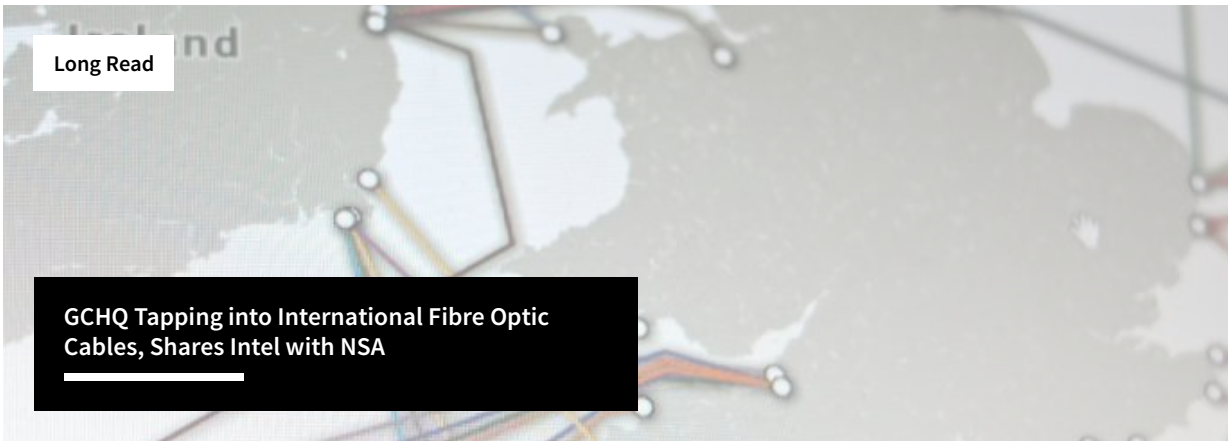
The Trap of Simplicity: Why Analogies for Surveillance Fail Us

Long Read

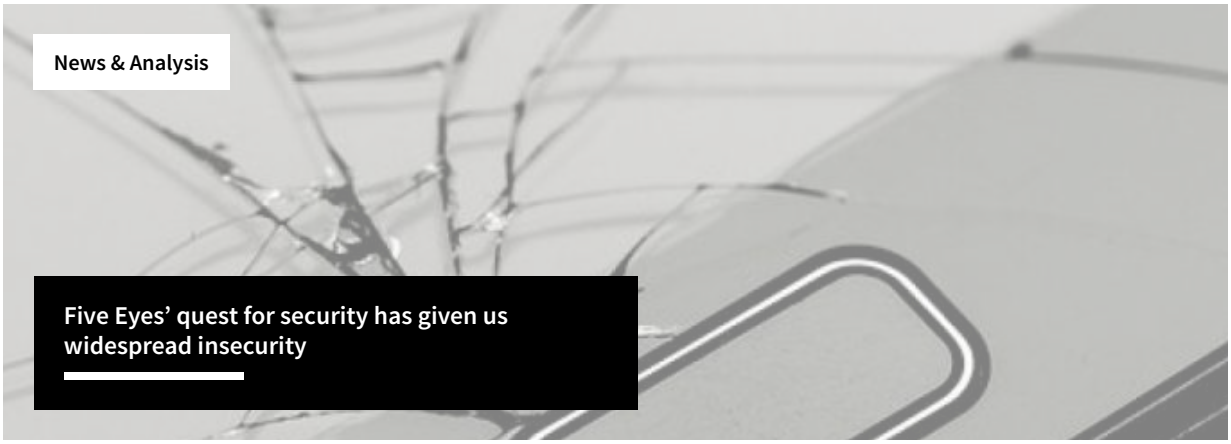


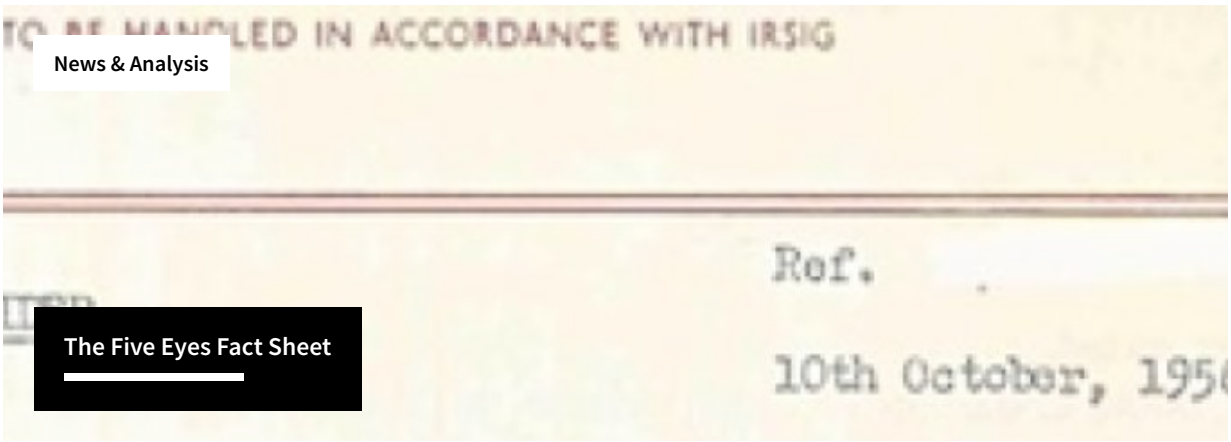
Report

Eyes Wide Open



News and Updates





Sign up for alerts about Privacy International's work on law, regulation and litigation.

Sign Up!

Legal Files

A. Disclosure

Attachment	Size
State Department (10 Oct. 2018)	4.24 MB
NSA (21 Sept. 2018)	5.72 MB
State Department (21 Sept. 2018)	189.58 KB
NSA (12 Sept. 2018)	5.87 MB

Attachment	Size
NSA (27 July 2018)	657.13 KB
Department of Defense (11 July 2018)	1.61 MB
NSA (11 May 2018)	3.88 MB
State Department (16 April 2018)	84.05 KB
NSA (6 April 2018)	2.91 MB
State Department (15 March 2018)	67.85 KB
State Department (15 Feb. 2018)	320.08 KB
State Department (2 Jan. 2018)	2.76 MB
State Department (4 Dec. 2017)	1.03 MB
State Department (2 Nov. 2017)	341.91 KB

B. U.S. District Court

Attachment	Size
Answer (21 Aug. 2017)	2.51 MB
Complaint (5 July 2017)	189.66 KB
Exhibit A to the Complaint (5 July 2017)	1.38 MB
Exhibit B to the Complaint (5 July 2017)	899.74 KB

Investigations and Research

Recent Campaigns

Why Privacy?

Financial

Privacy

Why We Use Your Data

How We Use Your Data

How We Learned

Why Cookies?!

Resources

What is GDPR?

Explainers

Invisible Manipulation Cases

Privacy Country Briefings

Hacking Safeguards

Surveillance Industry Index

Data Protection Guide

Contact Us

62 Britton Street,
London, EC1M 5UY
UK

Charity Registration No: 1147471

Click here to contact us.

Media: **press@privacyinternational.org**

UKUSA Agreement Release 1940-1956

Please Note: These historical documents are PDF images of formerly classified carbon paper and reports that have been declassified. Due to the age and po PDF images, a screen reader may not be able to process the images into word documents. In accordance with Section 504 of the Rehabilitation Act of 1973, may request that the government provide auxiliary aids or services to ensure effective communication of the substance of the documents. For such request Public Affairs Office at 301-688-6524.

The tradition of intelligence sharing between NSA and its Second party partners has deep and widespread roots that have been cultivated quarters of a century. During World War II, the U.S. Army and Navy each developed independent foreign SIGINT relationships with the Brit of Canada, Australia, and New Zealand. These relations evolved and continued across the decades. The bonds, forged in the heat of a wor decades of trust and teamwork, remain essential to future intelligence successes.

The March 5, 1946, signing of the BRUSA (now known as UKUSA) Agreement marked the reaffirmation of the vital WWII cooperation betwe and United States. Over the next 10 years, appendices to the Agreement, some of which are included with this release to the public, were These appendices and their annexures provide details of the working relationship between the two partners and also address arrangeme Second Parties (Australia, Canada, and New Zealand).

Release Contents

Early Papers (1940-1944)

- Early Papers Concerning US-UK Agreement - 1940-1944 (/Portals/70/documents/news-features/declassified-documents/ukusa/early_pa

1943

- Agreement between British Government Code and Cipher School and U.S. War Department in Regard to Certain "Special Intelligence" - (/Portals/70/documents/news-features/declassified-documents/ukusa/spec_int_10jun43.pdf)
- An Agreement between the U.S. Army and British CG and CS Concerning Cooperation in Matters Relating to Communication Intelligence (/Portals/70/documents/news-features/declassified-documents/ukusa/comms_int_23jun43.pdf)

1944

- U.S. - British R.I. ("BRUSA") Circuit - 7 Jan. 1944 (/Portals/70/documents/news-features/declassified-documents/ukusa/brusa_7jan44.pdf)
- U.S. - British R.I. ("BRUSA") Circuit: Instructions for Use - 14 March 1944 (/Portals/70/documents/news-features/declassified-documents/ukusa/brusa_14mar44.pdf)
- The BRUSA Circuit - Establishment Date - 29 April 1944 (/Portals/70/documents/news-features/declassified-documents/ukusa/brusa_29
- Memorandum for G.P.O. Watch Officers - BRUSA System - 23 June 1944 (/Portals/70/documents/news-features/declassified-documents/u

- BRUSA Traffic - 23 June 1944 (/Portals/70/documents/news-features/declassified-documents/ukusa/brusa_traffic_23jun44.pdf)
- OP-20-G Dispatch Traffic (Including BRUSA) - 26 June 1944 (/Portals/70/documents/news-features/declassified-documents/ukusa/op-20-
- British-U.S. Agreement on German and Japanese Projects - 4 July 1944 (/Portals/70/documents/news-features/declassified-documents/ukusa/german_japanese_proj_4jul44.pdf)
- An Agreement between GC & CS and Negat on Japanese Cryptanalytic Tasks - 23 Oct. 1944 (/Portals/70/documents/news-features/decla documents/ukusa/gc-cs-negat_23oct44.pdf)

1945

- Memorandum from Army-Navy Communications Intelligence Board (ANCIB) re: Signals Intelligence - 22 Aug. 1945 (/Portals/70/documer features/declassified-documents/ukusa/ancib_22aug45.pdf)
- Joint Meeting of ANCIB and ANCICC - 15 Oct. 1945 (/Portals/70/documents/news-features/declassified-documents/ukusa/joint_mtg_15o
- Joint Meeting of ANCIB and ANCICC - 29 Oct. 1945 (/Portals/70/documents/news-features/declassified-documents/ukusa/joint_mtg_29o
- Draft British-U.S. Communication Intelligence Agreement - 1 Nov. 1945 (/Portals/70/documents/news-features/declassified-documents/ukusa/draft_agrmt_1nov45.pdf)
- Joint Meeting of Army-Navy Communications Intelligence Board Joint Meeting Summary - 1 Nov. 1945 (/Portals/70/documents/news-features/declassified-documents/ukusa/joint_mtg_1nov45.pdf)

1946

- STANCICC Subcommittee on Intelligence and Security - 8 Jan. 1946 (/Portals/70/documents/news-features/declassified-documents/ukus
- STANCICC Ad Hoc Subcommittee for Technical Conference Planning Establishing of - 14 Jan. 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/STANCICC_14jan46.pdf)
- Draft British-U.S. Communications Intelligence Agreement Proposed Revision of - 15 Jan. 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/proposed_rev_15jan46.pdf)
- Draft British- U.S. Communications Agreement - Accepted by British - 16 Jan. 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/draft_accepted_16jan46.pdf)
- Draft British-U.S. Communications Agreement Referred by STANCIB for Approval - Not dated (/Portals/70/documents/news-features/de documents/ukusa/draft_for_app_notdated.pdf)
- Preparation and Delivery of Drafts of Tentative British-U.S. COMINT Agreement - 18 Jan. 1946 (/Portals/70/documents/news-features/de documents/ukusa/tentative_agree_18jan46.pdf)
- Appendix to BRUSA CI Agreement: British-U.S. COMINT Security and Dissemination Regulations - 22 Jan. 1946 (/Portals/70/documents/n features/declassified-documents/ukusa/appendix_brusa_ci_22jann46.pdf)
- British-U.S. Communications Intelligence Security and Dissemination Regulations - 30 Jan. 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/security_diss_regs_30jan46.pdf)
- Appendix to British-U.S. CI Agreement Regulations for the Coordination of Cryptanalysis Traffic Analysis and Associated Techniques - 5 F (/Portals/70/documents/news-features/declassified-documents/ukusa/appendix_ci_agree_5feb46.pdf)
- Appendix to British-U.S. CI Agreement - Regulations for the Coordination of the Exchange of Collateral Material - Not dated (/Portals/70/ features/declassified-documents/ukusa/appendix_ci_agree_notdated.pdf)
- Communications Intelligence - 8 Feb. 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/comms_int_8feb46.pd
- Copies of Draft Appendices to British-US CI Agreements - 12 Feb. 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/copies_draft_appendices_12feb46.pdf)
- Joint Meeting of STANCIB and STANCICC - 15 Feb. 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/STANCIB_
- U.S.-British Agreement and FBI Membership on STANCIB - 19 Feb. 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/fbi_stancib_19feb46.pdf)
- Appendices A-G to British-U.S. CI Agreement British - U.S. Communications Intelligence Security and Dissemination Regulations - 26 Feb (/Portals/70/documents/news-features/declassified-documents/ukusa/appendices_a-g_26feb46.pdf)
- STANCIB and STANCICC Joint Meeting - 27 Feb. 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/STANCIB_ST
- Corrections to BRUSA CI Appendices Dated 26 Feb. 1946 - 28 Feb. 1946 (/Portals/70/documents/news-features/declassified-

documents/ukusa/corrections_ci_appendices_28feb46.pdf)

- Corrections to BRUSA CI Appendices - 1 March 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/corrections_ci_appendices_1mar46.pdf)
- British-U.S. Communications Intelligence Agreement and Outline - 5 March 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/agreement_outline_5mar46.pdf)
- Minutes of the Inauguration Meeting British Signal Intelligence Conference - 11-27 March 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/minutes_inauguration_11mar46.pdf)
- Final Recommendation of the Technical Conference 11-27 March 1946 (/Portals/70/documents/news-features/declassified-documents/ukusa/final_rec_tech_conf_1mar46.pdf)

1948

- Appendices to U.S.-British Communications Agreement - 15-26 July 1948 (/Portals/70/documents/news-features/declassified-documents/ukusa/appendices_jul48.pdf)
- Tabular Comparison of 1946 and 1948 Appendices to U.S. - British COMINT Agreement (/Portals/70/documents/news-features/declassif documents/ukusa/tabular_comparison.pdf)

1951-1953

- UKUSA COMINT Agreement and Appendices Thereto (/Portals/70/documents/news-features/declassified-documents/ukusa/ukusa_com
- BRUSA Planning Conference Final Report (/Portals/70/documents/news-features/declassified-documents/ukusa/brusa_final_rep_1953.p

1956-1961

- New UKUSA Agreement - 10 May 1955 (/Portals/70/documents/news-features/declassified-documents/ukusa/new_ukusa_agree_10may
- Classification and Handling of Information Related to COMINT or COMINT Related Activities; Appendix B; Annexure B3 5 October 1959 (/Portals/70/documents/news-features/declassified-documents/ukusa/classification_and_handling_of_information_related_to_comint_or_comint_activities_appendix_b_annexure_b3_5_octo
- Principles of Security and Dissemination; Appendix B 1 July 1959 (/Portals/70/documents/news-features/declassified-documents/ukusa/principles_of_security_and_dissemination_appendix_b_1_july_1959.pdf)
- Principles of UKUSA Collaboration with Commonwealth Countries Other Than the UK; Appendix J 13 February 1961 (/Portals/70/docume features/declassified-documents/ukusa/principles_of_ukusa_collaboration_with_commonwealth_countries_other_than_the_uk_appendix_j_13_february_1961
- Security Principles Governing the Conduct of COMINT Operations in Exposed Areas; Appendix B; Annexure B2 21 March 1960 (/Portals/ features/declassified-documents/ukusa/secrutiy_principles_governing_the_conduct_of_comint_operations_in_exposed_areas_appendix_b_annexure_b2_21_n
- The Assignment of COMINT to Categories and Sub-Categories; Appendix D; Annexure B1 1 July 1959 (/Portals/70/documents/news-featu documents/ukusa/the_assignment_of_comint_to_categories_and_sub-categories_appendix_d_annexure_b1_1_july_1959.pdf)
- Types of Information to be Given the Same Protection as COMINT; Appendix B; Annexure B3; Annex A 1 January 1959 (/Portals/70/docu features/declassified-documents/ukusa/types_of_information_to_be_given_the_same_protection_as_comint_appendix_b_annexure_b3_annex_a_1_january_1
- Types of Information to be Handled via COMINT Channels Only; Appendix B; Annexure B3; Annex B; 1 January 1959 (/Portals/70/docum features/declassified-documents/ukusa/types_of_information_to_be_handled_via_comint_channels_only_appendix_b_annexure_b3_annex_b_1_january_1959
- Types of Information Which May be Handled in Accordance with Normal Security Regulations; Appendix B; Annexure B3; Annex C 1 Janu (/Portals/70/documents/news-features/declassified-documents/ukusa/types_of_information_which_may_be_handled_in_accordance_with_normal_security_regulations_appendix_b_annexu

Skip to main content (Press Enter)

ver=2018-08-08-105310-530)

- UKUSA Arrangements Affecting Australia and New Zealand; Appendix J; Annexure J1 13 February 1961 (/Portals/70/documents/news-fea documents/ukusa/ukusa_arrangements_affeecting_australia_and_new_zealand_appendix_j_annexure_j1_13_february_1961.pdf)

ACTING CHIEF
POLICE COORDINATION STAFF

31 October 1972

Dr. Tordella

You may be interested in a quick review of the attached problems by Fred Gruber which call for help.

D. D. Chapin

Encl:
a/s

Doc [illegible]

~~TOP SECRET~~

TO: Mr. Harold H. Gallaher
NSAFC, J4
RC-11478/72

FROM: Mr. Fred Griffin
30 October 1972

Col. Ellis on the Fritz group is [illegible]
Capone and Scott. Since the memos are in the
open, how is Kissinger going to [illegible]
in the weekly reference sheets for feeding
Dr. Kissinger? Yes.

Ltj

HANDLE VIA COMINT CHANNELS

WARNING

This document contains classified information affecting the national security of the United States within the meaning of the espionage laws, US Code, Title 18, Sections 793, 794, and 798. The law prohibits the transmission or the revelation of its contents in any manner to an unauthorized person, as well as its use in any manner prejudicial to the safety or interest of the United States or the benefit of any foreign government to the detriment of the United States.

THIS DOCUMENT MUST BE KEPT IN COMMUNICATIONS INTELLIGENCE CHANNELS AT ALL TIMES

It is to be seen only by U.S. personnel especially indoctrinated and authorized to receive COMMUNICATIONS INTELLIGENCE information, and its security must be maintained in accordance with COMMUNICATIONS INTELLIGENCE REGULATIONS.

No action is to be taken on any COMMUNICATIONS INTELLIGENCE which may be contained herein, regardless of the advantages to be gained, unless such action is first approved by the Director of Central Intelligence.

~~TOP SECRET~~

TOP SECRET

~~TOP SECRET~~

~~HANDLE VIA COMINT CHANNELS~~

SC-11478/72

27 October 1972

MEMORANDUM FOR THE RECORD

SUBJECT: Historical Note on the USCIB COMINT Agreement

1. The question occasionally arises as to the governmental levels at which the USCIB COMINT Agreement was authorized or approved. The attached documents show that the President of the United States authorized an agreement in this field, and that the British Foreign Minister must have been aware of it.

2. Attachment A is a copy of a Presidential Memorandum, dated 29 September 1945, authorizing the continuation of wartime U.S.-British "collaboration in the field of communication intelligence."

3. Attachment B is a copy of an 8 February 1946 page from the notebook which formed the principal basis for the published diaries of the late Secretary of Defense Forrestal. The account of the meeting contained in this excerpt shows the high levels of the U.S. at which the Agreement was considered, and suggests that Secretary of State Byrnes had discussed the matter with British Foreign Secretary Bevin.

4. Attachment C is a copy of the account of the above-mentioned meeting as it appeared in the published Diaries. At the request of the Department of State, the editors deleted all references to communications intelligence and Sir Edward Travis. They developed an innocent introductory sentence, omitted the first paragraph, and changed the subtitle from "Communications Intelligence" to "Meeting." (Not pertinent to this discussion, but of some editorial interest, is the deletion of "but" from the sixth line of the original notebook.)

BY IMPDET
CL BY 003838

~~TOP SECRET~~

~~HANDLE VIA COMINT CHANNELS~~

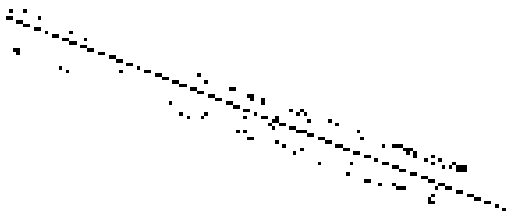
5. The UKUSA Agreement was ultimately signed on 5 March 1946 by Col. Patrick Maxwell-Johnson, British Army General Staff, for and in behalf of the London Signal Intelligence Board (LSIB), and by Lt. Gen. Hoyt S. Vandenberg, USA, Senior Member, for and in behalf of the State Army Navy Communications Board (SANACB). The parties to the Agreement are described as SIGINT, "(representing the U. S. State, Navy, and War Departments and all other U. S. Communication intelligence authorities which may function)" and ISIS "(representing the Foreign Office, Admiralty, War Office, and all other British Empire Communication Intelligence authorities which may function)."

6. Obviously, these parties and signatories were themselves hardly operating at a purely diplomatic level; however, the documents contained in the attachments show that they were not working unilaterally or without authority and approval at the highest levels.

(signed) Fred Taub

FRED TAUB
Historical Officer
Division D

Doc ID 6619447



~~TOP SECRET~~

MEMORANDUM FOR:

The Secretary of State
The Secretary of War
The Secretary of the Navy

The Secretary of War and the Secretary of the Navy are hereby authorized to direct the Chief of Staff, U. S. Army and the Commander in Chief, U. S. Fleet, and Chief of Naval Operations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States.

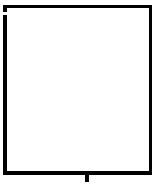
/s/ Harry S. Truman

12 September 1946

~~TOP SECRET~~

Doc ID: 1063615

~~TOP SECRET~~



December 1935

DESCRIPTION OF
SIGINT RELATIONS BETWEEN NSA AND [illegible]

~~AUTHORITY TO CLASSIFY IS~~
~~DERIVED FROM~~ ~~DECLASSIFY ON:~~ ~~X1~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~LIMITED DISTRIBUTION~~

~~TOP SECRET~~

TABLE OF CONTENTS

I. INTRODUCTION

The following is a review of the NSA-GCHQ SIGINT relationship including an assessment of the present value of the exchange and identifies problems. This review is intended to serve as a basis for determining our plans for the conduct of this relationship in the future, for any improvements/changes regarding control and accountability of the existing exchange, as well as developing proposals for additional contributions which should be made by each party. (U)

II. FINDINGS/CONCLUSIONS

There is a heavy flow of raw intercept, technical analytic results, and SIGINT product between NSA and GCHQ, to include direct distribution of product to each party to [illegible] (TS-CCO)

[redacted]

III. DISCUSSION

- General

The BRUSA collaboration with the UK began in 1941 and was formalized in the UKUSA Agreement of 1946 contained in Annex B1. It has developed into one of virtually full partnership and interdependence, to include combined working parties, joint operations, the exchange of liaison and assignment of analysts to integrated posts. In addition, divisions of effort (COCE) and/or understandings between NSA and GCHQ are undertaken to expand or existing requirements. Each country makes unique contributions, and while the U.S. has moved far ahead in total resources committed and in technology development, the contribution of the UK continues to be of great value. (U-CCO)

- U-USA Agreement and Appendices

The UKUSA Agreement, dated 5 March 1946, has twelve short paragraphs and was so generally written that, with the exception of a few broad areas, no changes to it have been made. It was signed by a UK representative of the London Signals Intelligence Board and the U.S. Senior Member of the State-Army-Navy Communications Intelligence Board (a predecessor organization which evolved to be the present National Foreign Intelligence Board). The principles remain sound, allowing for a full and independent partnership. In effect, the basic agreement allows for the exchange of all COMINT results including end product and pertinent raw data from each partner for targets worldwide, unless specifically excluded from the agreement at the request of either party. It also makes provision for restricting exchange of material when it is of special interest to either party, but notes that such exceptions should be kept to an absolute minimum. Over the years this has been the case. Additionally, the agreement makes provision for obtaining agreement between the two partners for COMINT relationships established with Third Parties and to ensure that materials received from such Third Party arrangements are made available to GCHQ and NSA. Provision was made to give special consideration to COMINT agencies of British Dominions (e.g., what are now Canada, Australia, New Zealand and to not consider them as Third Parties). Over the years numerous appendices have been added to cover specific areas of mutually interest and exchange/dissemination sophistication. The appendices to the UKUSA Agreement address such items as principles of security and dissemination, principles of relationships with Third Parties, standardization of intercept formats, common classification and categorization criteria,

exchange of material obtained through clandestine or covert sources, and principles of UKUSA collaboration with commonwealth countries. [A listing of each appendix with an explanatory comment is included as Annex B.] (TS-CCO)

- Italian

In accordance with Appendix E of the UKUSA Agreement, NSA and GCHQ maintain a liaison officer in each other's country to facilitate SIGINT collaboration. In the UK, the U.S. officer is the Special U.S. Liaison Officer, London (SUSLOL) and in Washington the UK officer is the Senior UK Liaison Officer, Washington, D.C. (SUKLOW). Although SUSLOL represents the National Foreign Intelligence Board (NFIB) as well as NSA in all SIGINT relationships with the UK, the liaison staffs [redacted] have similar/qualified people who can liaise with the major key components of each agency as well as the major operational production groups, a cryptanalytic expert, and necessary administrative and communications support personnel. SUSLOL and SUKLOW and their respective staffs protect the official interests of whatever two national centers, as well as provide SIGINT support to their national/crypto.

[redacted]

HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET

[redacted]

- Integrated Analysis

NSA and [redacted] have assigned cryptologic specialists into each other's IO operational elements for purposes of combined operations on select target problems, acquiring experience and training, and for contributing unique special talent as well. This promotes almost complete access to [redacted] by these integrated analysts in the areas where they are assigned. [redacted]

- Targeted Operations

[redacted]

[redacted]

Other Areas of Combined Operations or Integrated Operations

The United States and UK have SIGINT personnel assigned to various overseas field sites of each other. These include the following:

Site		Number of People Assigned		Comment
UK	U.S.	UK	U.S.	

- Exchange of Visitors

A great number of visits are exchanged between the two national SIGINT HQ at each party representing various levels of personnel from the Directorate Down. These visits take on different forms, e.g., analyst-to-analyst discussions, conferences, periodic meetings, management/planning reviews

and consultations, Directorate level policy decisions.

- Major Conference Exchanges

There are many conferences held between NSA and GCHQ which cover a multitude of topics. Most are held on an annual basis and usually alternate meeting places between the two sanlocs. The more significant conferences include the following:

Conference	Comments
Program Management & Review	Senior Management participation
Joint Management Review	Senior Management (at Deputy Director level) participation

- Communications Tie-ins

Other than CAIICOM and mail correspondence, CINC and USA have various means for communications with each other. There are several CAIICOM circuits between the two sites.

- Computer Hook-ups/Accessibility

- Technology Exchange

There is [illegible] technology exchange between both centers.

[redacted]

IV. VALUE OF RELATIONSHIP

- The value of this relationship is high and allows for a much faster, higher effect than is possible with only U.S. resources. [redacted]

[redacted]

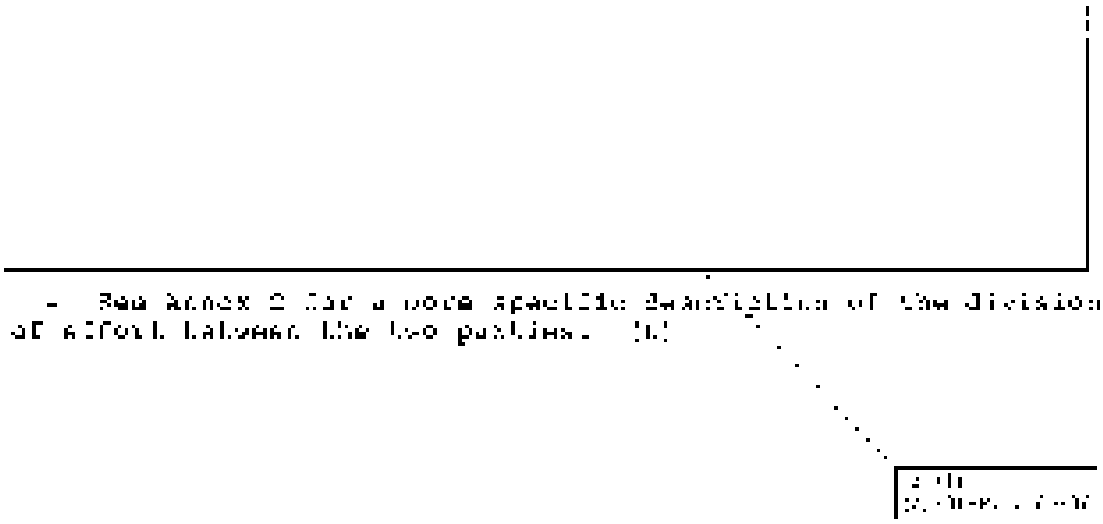
- SCHQ is a contributor to our cryptanalytic efforts.

V. PROBLEMS

VI. BASES OF COOPERATION/AGREEMENT

- The SIGAD-MUSCULAR exchange involves a sharing of a wide variety of targets worldwide, spanning both military activities and terrorist activities, and it involves all forms of SIGINT, i.e., COMINT, FISINT, and TISINT. This arrangement includes the exchange of material from intercept, analytic, processing

- Cooperation between NSA's and GCHQ's personnel has been extensive; however, a significant amount of division of effort is accomplished without any formal SOP or MOU and has evolved through cooperation engendered by personal contacts and exchanges. An infrastructure is created on each target of mutual interest in terms of collection, processing and exploitation.



- See Annex 2 for a more specific examination of the division of effort between the two positions. [1]

ANNEXES: A UKUSA AGREEMENT OF 1946 - (S)

B LISTING OF APPLICABLE MOD THE UKUSA AGREEMENT (S)

C DEFINITIONS OF UKUSA DIVISION OF EFFORT (U)

D PRINCIPAL UK CRYPTOLOGIC INSTALLATIONS (S)

E U.S. CRYPTOLOGIC AGENCIES IN THE UK (S)

[redacted]

[redacted]

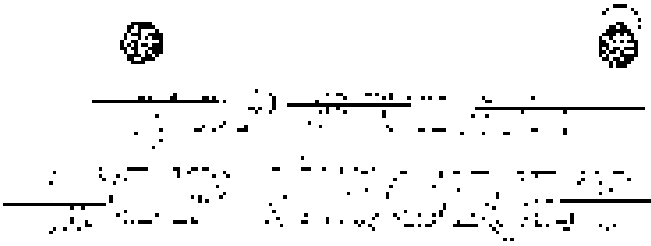
[redacted]

TOP SECRET

UKUSA SECURITY AGREEMENT

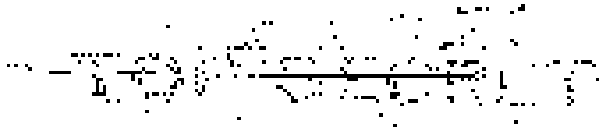
5 March 1946

TOP SECRET



INDEX OF

BRITISH-U.S. COMMUNICATION INTELLIGENCE AGREEMENT



[illegible] SIGINT AGREEMENT

1. [illegible] Agreement.

The following agreement is made between the [illegible] (hereinafter the U. S. Signals Intelligence Agency) [illegible] the U. S. State, Navy, and War Departments, and [illegible] U. S. Communications Intelligence activities which may [illegible] and the London Signal Intelligence [illegible] Foreign Office, Admiralty, War Office, Air Ministry, and all other British Empire Communication Intelligence activities which may function).

2. [illegible] Agreement.

The agreement governs the relations of the above-mentioned parties in Communication Intelligence only. However, the exchange of such collateral material as is applicable for technical purposes and is not prejudicial to national interests will be effected between the Communication Intelligence agencies of both countries.

3. [illegible] Agreement.

It is agreed that each agency will exchange Intelligence information to employ all processes involved in the collection, production, and dissemination of information derived from the communications of other nations.

For the purposes of this agreement British Empire is understood to mean all British territory under one jurisdiction.

4. [illegible]

5. [illegible]

Doc ID: 6710634

[redacted]

3. 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 facilities and equipment

(3) traffic analysis

(4) cryptanalysis

(5) decryption and translation

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

[redacted]

As used in this agreement foreign communications are understood to mean all communications of a government or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor, and shall include commercial communications of a foreign country which may contain information of military, political, or economic value. Foreign country as used herein is understood to include any country, whether or not the government is recognized by the U. S., or the British Empire, excluding only the U. S., the British Commonwealth of Nations, and the British Empire.

[redacted]

(c) Each exchange will be undertaken on all such undertakings may not specifically excluded from the Agreement at the request of either party [illegible] the Agreement [illegible] the [illegible] of such party to [illegible] the [illegible] and to exercise no jurisdiction over [illegible] and wholly agents upon [illegible]

4. Extent of the Agreement - Methods and Techniques

(a) The exchange by the Agencies of the following categories of methods and techniques involved in the operations outlined in paragraph 3(a):

(b) Each exchange will be understood as all such [illegible], except that upon request of the other party information may be withheld by either party when the special circumstances so require. Such notification will indicate a description of the information being withheld, sufficient to the satisfaction of the withholding party, to convey its significance. It is the intention of both parties to limit such exceptions to the [illegible] minimum.

5. United Parties to the Agreement

Both parties will regard this agreement as precluding action with third parties on any subject appertaining to Communications Intelligence except in accordance with the following understandings:

Throughout this agreement [illegible] parties are understood to mean all individuals or authorities other than those of the United States, the British Empire, and the British Dominions.

(c) It will be necessary to this Agreement to permit its existence to any third party whatsoever.

(b) Each party will seek the agreement of the other to any action with mutual profits, but will have no such action until the advisability is agreed upon.

(c) The agreement of the other having been obtained, it will be left to the party concerned to carry out the agreed action in the most appropriate way, without obligation to disclose precisely the channels through which action is taken.

(d) Each party will observe that the rights of any such action are only available to the other.

5. The Relations

(a) While the Institutions are not parties to this Agreement, they will not be registered as third parties.

(b) The London STOCK Board will, however, keep the U. S. informed of any arrangements or proposed arrangements with any Institution mentioned.

(c) STOCK will make no arrangements with any Designated Agency other than Canadian except Ireland, or with the prior approval of, the London STOCK Board.

(d) As regards Canada, STOCK will consult in accordance with any Agency therein without first obtaining the views of the London STOCK Board.

(e) It will be established on any Decision agreed with them as Institutions takes place with

that agreed in the terms of paragraphs 5, 6, and 8 of this agreement and to the arrangements laid down in paragraph 7.

7. Channels between U. S. and British Empire Agencies

(a) STANCIB will make no arrangements in the sphere of Communication Intelligence with any British Empire agency except through, or with the prior approval of, the London SIGINT Board.

(b) The London SIGINT Board will make no arrangements in the sphere of Communication Intelligence with any U. S. agency except through, or with the prior approval of, STANCIB.

8. Dissemination and Security

Communication Intelligence and secret or above technical matter exchanged hereunder will be disseminated in accordance with identical security regulations to be drawn up and kept under review by STANCIB and the London SIGINT Board in collaboration. Within the terms of these regulations dissemination by either party will be made to U. S. recipients only as approved by STANCIB; to British Empire recipients and to Dominion recipients other than Canadian only as approved by the London SIGINT Board; to Canadian recipients only as approved by either STANCIB or the London SIGINT Board; and to third party recipients only as jointly approved by STANCIB and the London SIGINT Board.

9. Dissemination to Commercial Concerns

STANCIB and the London SIGINT Board will ensure that without prior notification and consent of the other party in each instance no dissemination of information derived from Communication Intelligence sources is made to any individual or agency, governmental or otherwise, that will exploit it for commercial purposes.

10. Previous Agreements

This Agreement supersedes all previous agreements between British and U. S. authorities in the Communication Intelligence field.

11. Amendment and Termination of Agreement

This Agreement may be amended or terminated completely or in part at any time by mutual agreement. It may be terminated completely at any time on notice by either party, should either consider its interests best served by such action.

12. Activation and Implementation of Agreement

This Agreement becomes effective by signature of duly authorized representatives of the London SIGINT Board and STANCIB. Thereafter, its implementation will be arranged between the Communication Intelligence authorities concerned, subject to the approval of the London SIGINT Board and STANCIB.

For and in behalf of the London Signal Intelligence Board:

Patrick Marr-Johnson
Colonel, British Army General Staff

For and in behalf of the State-Army-Navy Communication Intelligence Board:

Hoyt S. Vandenberg
Lieutenant General, USA
Senior Member

5 March 1946

~~TOP SECRET~~

~~TOP SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

[illegible]

[illegible] AGREEMENT [illegible] MAY BE AMENDED
[illegible]

[illegible]

APPENDIX A - [illegible]

APPENDIX B - [illegible]

APPENDIX C - [illegible]
Quality [illegible]

APPENDIX D - [illegible]

APPENDIX E - [illegible]

APPENDIX F - [illegible]
[illegible]

APPENDIX G - [illegible]
[illegible]

APPENDIX H - [illegible]
[illegible]

APPENDIX I - [illegible]

APPENDIX J - [illegible]
[illegible]

APPENDIX K - [illegible]
[illegible]

[illegible] [illegible] [illegible], [illegible], [illegible]
[illegible]

APPENDIX L - [illegible]

APPENDIX M - [illegible]
[illegible]

APPENDIX N - [illegible]
[illegible]

APPENDIX O - [illegible]
[illegible]

APPENDIX P - [illegible]
[illegible]

APPENDIX Q - [illegible]
[illegible]

APPENDIX R - [illegible]
[illegible]

[illegible]

TOP SECRET

UNCLASSIFIED TO THE ATTACHED

A listing of arrangements which govern the relationship between the U.S. and U.K. COMINT Agencies, including statements of exchange, liaison, standardization, allocation of resources, telecommunication, review of hypothesis.

APPENDIX A - PLAN OF ATTACK

A definitive listing of those placed on the provisions of the Agreement.

APPENDIX B - PRINCIPLES OF SECURITY AND DISSEMINATION

Defines a number of terms peculiar to the COMINT agreements, specifies the considerations for assigning COMINT to categories; establishes basic security principles governing collection, access, dissemination, and communication; sets out all possible sources of COMINT.

APPENDIX C (SECURITY CATEGORIES) - THE ASSIGNMENT OF COMINT TO CATEGORIES AND SUB-CATEGORIES

This annex establishes the basis for (a) the establishment of sub-categories, (b) the assignment of COMINT to categories and sub-categories, and (c) the classification of COMINT assigned to categories and sub-categories, and (d) the application of controls to categories and sub-categories. It does not establish the detailed categorization of all COMINT, but does set out the criteria described in Annex B, to provide the organization and machinery of current review by agreed lines to facilitate the precise assignment of all COMINT categories and sub-categories.

APPENDIX D (HANDLING OF - SECURITY PROCEDURES APPLICABLE TO THE HANDLING OF COMINT, INCLUDING LIAISON WITH THIRD PARTIES)

This section defines secured areas, entry situations, dangerous situations, and hazardous activities. It sets up safeguards for communications and provides for the evacuation of COMINT equipment in a grave crisis or in risky or dangerous situations.

APPENDIX E (SECURITY OF - STANDARDIZATION AND PROCEDURES OF A SECURITY NATURE RELATED TO COMINT OR COMINT ACTIVITIES)

This annex establishes minimum standards with respect to the handling and classification of information which is derived COMINT or that contained in technical material or documents that reveal actual or prospective success or effort concerning the production of COMINT.

TOP SECRET

[illegible] reveals directly or by implication the existence or nature of COMINT or of COMINT activities.

APPENDIX B ANNEXURE B1 ANNEX A - TYPES OF INFORMATION TO BE GIVEN THE SAME PROTECTION AS COMINT

Lists the information which is neither COMINT nor "technical material" but which must be accorded the same protection of the classification and safeguard of the highest category of COMINT to which it relates.

APPENDIX B ANNEXURE B1 ANNEX B - TYPES OF INFORMATION TO BE HANDLED VIA COMINT CHANNELS ONLY

This Annex prescribes the classification and handling procedures for information that does not require codeword protection, but which relates to COMINT or COMINT activities.

APPENDIX B ANNEXURE B1 ANNEX C - TYPES OF INFORMATION WHICH MAY BE HANDLED IN ACCORDANCE WITH NORMAL SECURITY REGULATIONS

Discusses the types of information pertaining to COMINT which requires neither codeword protection nor the caveat "HANDLE VIA COMINT CHANNELS ONLY" and 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.

APPENDIX C - DESIGNATION OF INTERCEPT TARGETS

Outlines the [illegible] case numbering system for describing intercept targets in all fields other than International Commercial, for which a separate system is noted.

APPENDIX D - CO-ORDINATION OF TRAFFIC ANALYSIS AND EXCHANGE OF TRAFFIC ANALYSIS MATERIAL

Provides guidelines for the exchange of T/A materials and for coordination of intercept control to minimize duplication.

APPENDIX D ANNEXURE D1 - SPECIAL ARRANGEMENTS AGREED AT THE [illegible] [illegible]

Doc ID: 3965905

TOP SECRET

ANNEX E - CONFIDENTIALITY OF, AND ACCESS TO, INFORMATION OBTAINED FOR INTELLIGENCE PURPOSES

A statement of the principles governing accreditation of, and exchange of communication, cryptanalysis and associated techniques, including downgrading of system classification, status of weekly, allocation of codes methods, technical products, crypto intelligence and transfer of devices and personnel.

APPENDIX 1 TO ANNEX E - CRYPTO AGREEMENTS MADE AS FAR AS THIS COMMAND IS CONCERNED BY HIGHER AUTHORITY

Details of agreements for internal allocation of cryptanalytic tasks, etc. and reference to any special considerations, e.g. to prevent a wide and premature use of System Identification Sheets, transmission of the Master File and separation of the Cryptanalytic Status Records.

APPENDIX 2 - PROCEDURE TO BE FOLLOWED IN DISCLOSURE AND DISSEMINATION OF COMINT

Provides guidance as to classification of codes and sources of communications and for restrictions current on COMINT which is exchanged.

APPENDIX 3 - PROCEDURE TO BE FOLLOWED WHEN THERE IS DANGER OF COMINT FALLING INTO UNAUTHORIZED HANDS

Provides additional guidance beyond that in paragraphs 8 and 9 of the Agreement as to the handling of intercepted material and COMINT documents threatened with capture or overrun.

ANNEX F - SECURITY

Provides general guidance as to classification of material, communications, maintenance and protection of equipment, cryptographic aids, couriers or bag routes, distribution and accountability.

APPENDIX TO ANNEX F - SECURITY REGULATIONS APPLICABLE TO THE U.S. COMMUNICATIONS INTELLIGENCE ACTIVITY

Advances the security rules that

1. U.S. Citizens and U.S. Nationals are prohibited in the U.K.
2. Communications arrangements for visitors and couriers between the U.K.
3. U.S. Nationals placed attached to British controlled territory and British Nationals placed attached to U.S. controlled territory.

Doc ID 6490013

5. [redacted]
6. [redacted]
7. Other combined communication Area and Zones (existing and planned)

APPENDIX I - LIST OF ABBREVIATIONS

[redacted]

APPENDIX J - DIRECTIVE OF [redacted] CONFIGURATION MANAGEMENT (CM) OF [redacted] SYSTEMS

[redacted]

APPENDIX K ANNEX XI - [redacted] ARCHITECTURE AUDIT AND [redacted]

Self-explanatory.

[redacted]

APPENDIX L - [redacted] [redacted]

[redacted]

APPENDIX M ANNEXURE XI - [redacted] ARCHITECTURE PROCESS AT THE [redacted] [redacted] OF APPENDIX X

[redacted]

APPENDIX N - [redacted]

[redacted]

TOP SECRET

ANNEX A TO ANNEX [illegible] - [illegible]

This annex sets up objectives and general principles of coverage for nearby site surveys in the contiguous area (north of the 55th parallel).

APPENDIX A - PROCEDURE OF [illegible] AND IDENTIFICATION OF NAV. CONTROL POINTS

Rules of procedure and a standard format are used in the exchange of new point(s).

APPENDIX B TO ANNEX A - MODIFY SURVEYS AS REQUIRED AT THE [illegible] (Copy to be used for [illegible])

Consists of exhibits on the geodetic datum formats or layout for various kinds of new tracts.

APPENDIX B - ARRANGEMENTS FOR [illegible] OF CONTROL POINTS

This section describes conditions and situations under which coverage extension of either or both U.S. and U.K. COUNTRY units is desirable and specifies the responsibilities of the several parties if such an event has arisen.

APPENDIX A TO [illegible] - [illegible] OF U.S. AND U.K. OTHER UNITS - [illegible] OF EQUIPMENT

Directives responsibility for providing necessary assistance to [illegible] units might have to be relocated on an emergency basis.

[illegible]

A listing of the various U.S. and U.K. COUNTRY units located on territory controlled by the other party.

APPENDIX A - [illegible] ARRANGEMENTS FOR [illegible] [illegible] [illegible]

Self-explanatory.

[illegible]

[redacted]

[redacted]

Provides for liaison and exchange of personnel, coordination of intercession and exchange of intercepted texts between the 10th MI Unit Germany and the U.S. and U.K.

[redacted]

Basic principles governing COMINT arrangements by the U.K. and U.S. with third parties.

[redacted]

Definitions of terms used in Appendix B.

[redacted]

A statement of principles governing the international, or distributed, production of COMINT, which is agreed to be provided to the Allied Command Europe (ACE) as both parties and ways.

[redacted]

A statement of principles governing international, or distributed, production of COMINT which is agreed to be provided to Allied Command Europe (ACE) by both parties and ways.

[redacted]

A set forth of principles on product COMINT collaboration between the U.S. and U.K. as part of [redacted]

[redacted]

This memorandum is the formal agreement between the Director of the participating organizations in connection with matters and the Commander of the Combined Center Europe (CCE).

[redacted]

Classification: [redacted]

[redacted]

[redacted]

Describes steps to be taken in the event of hostilities involving the U.S., U.K., Canada, Australia, and New Zealand to ensure the greatest possible consideration be given to the completion, with security, of existing classified communications Terminal (CCITT) Circuits.

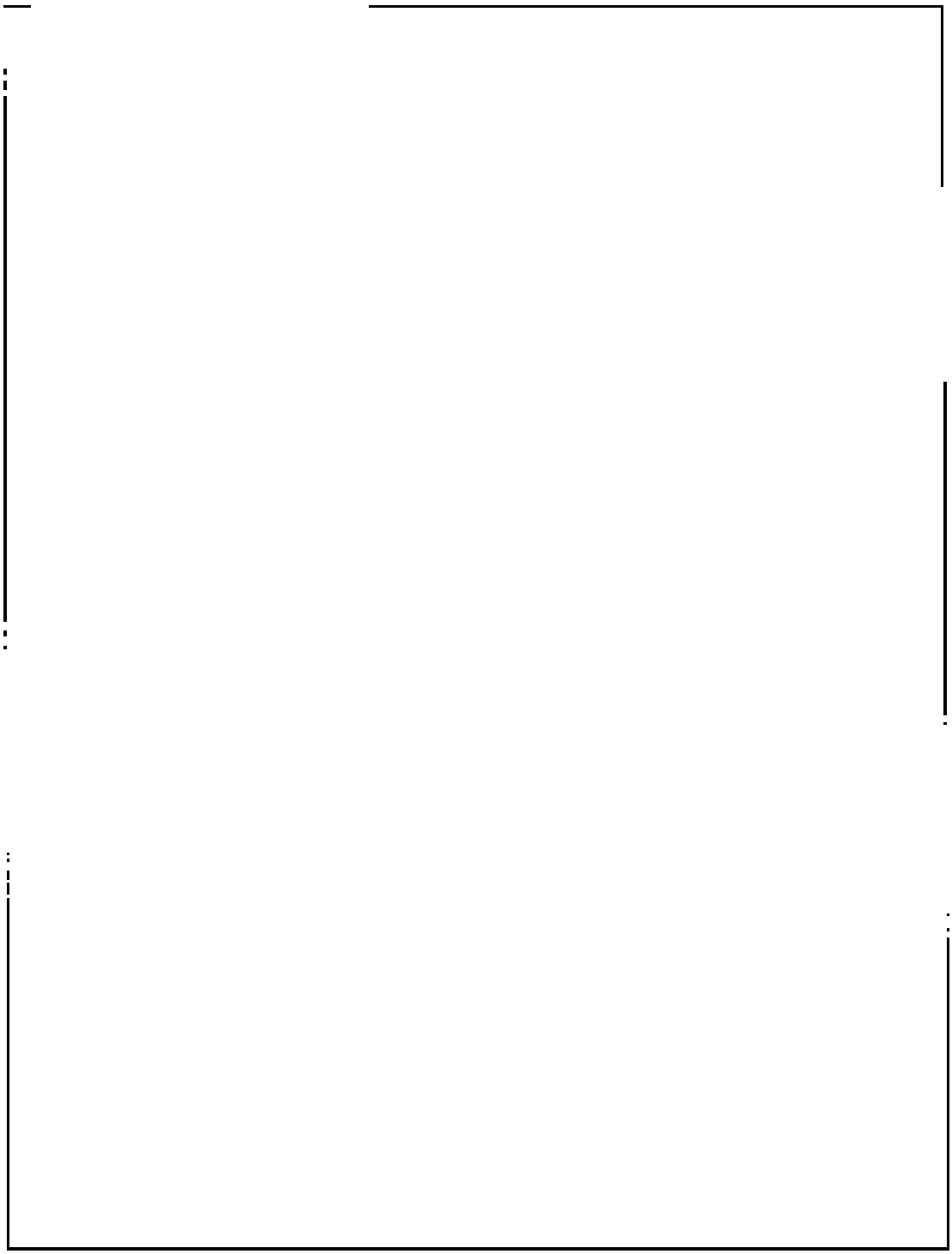
[redacted]

[redacted]

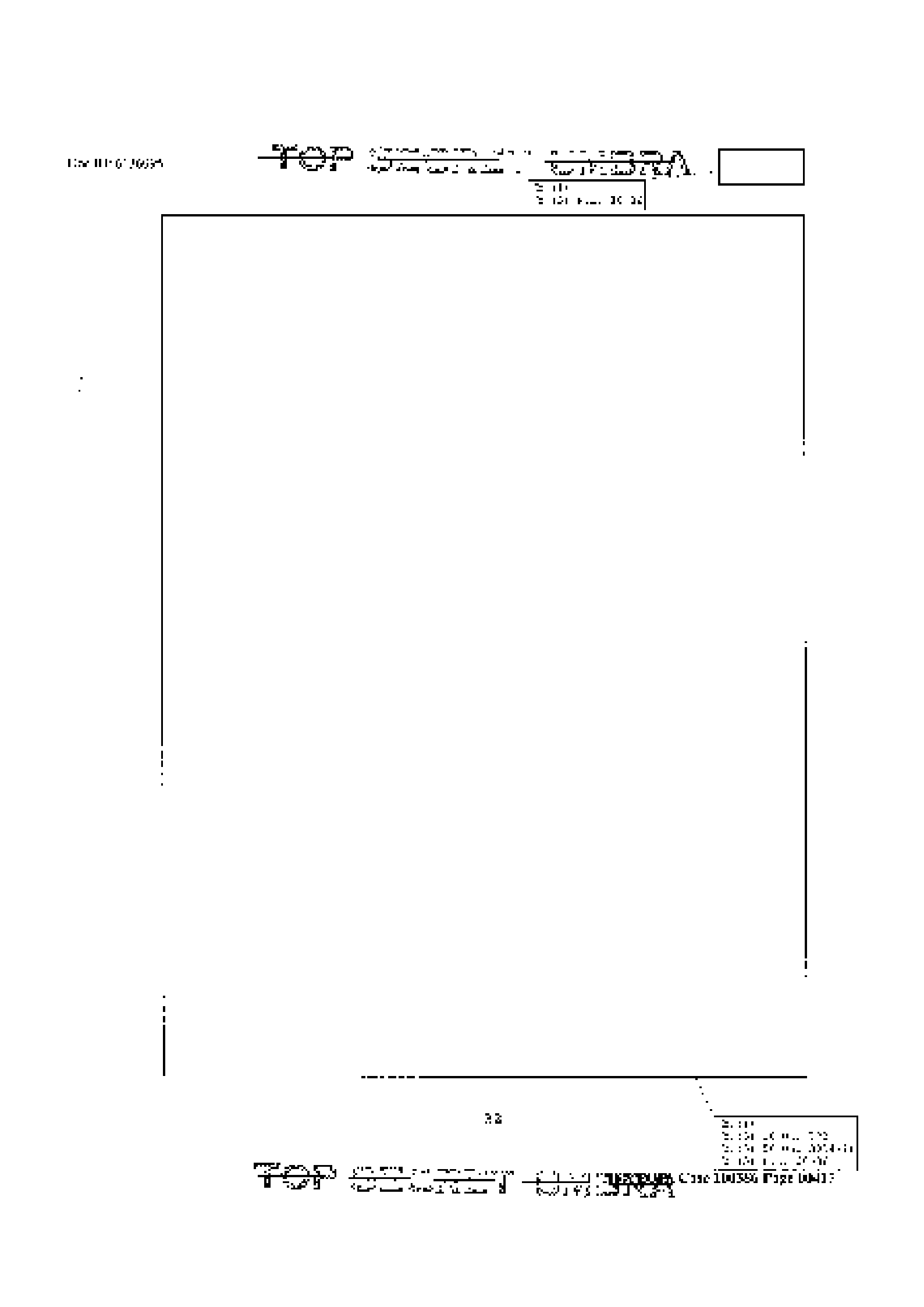
APPENDIX C

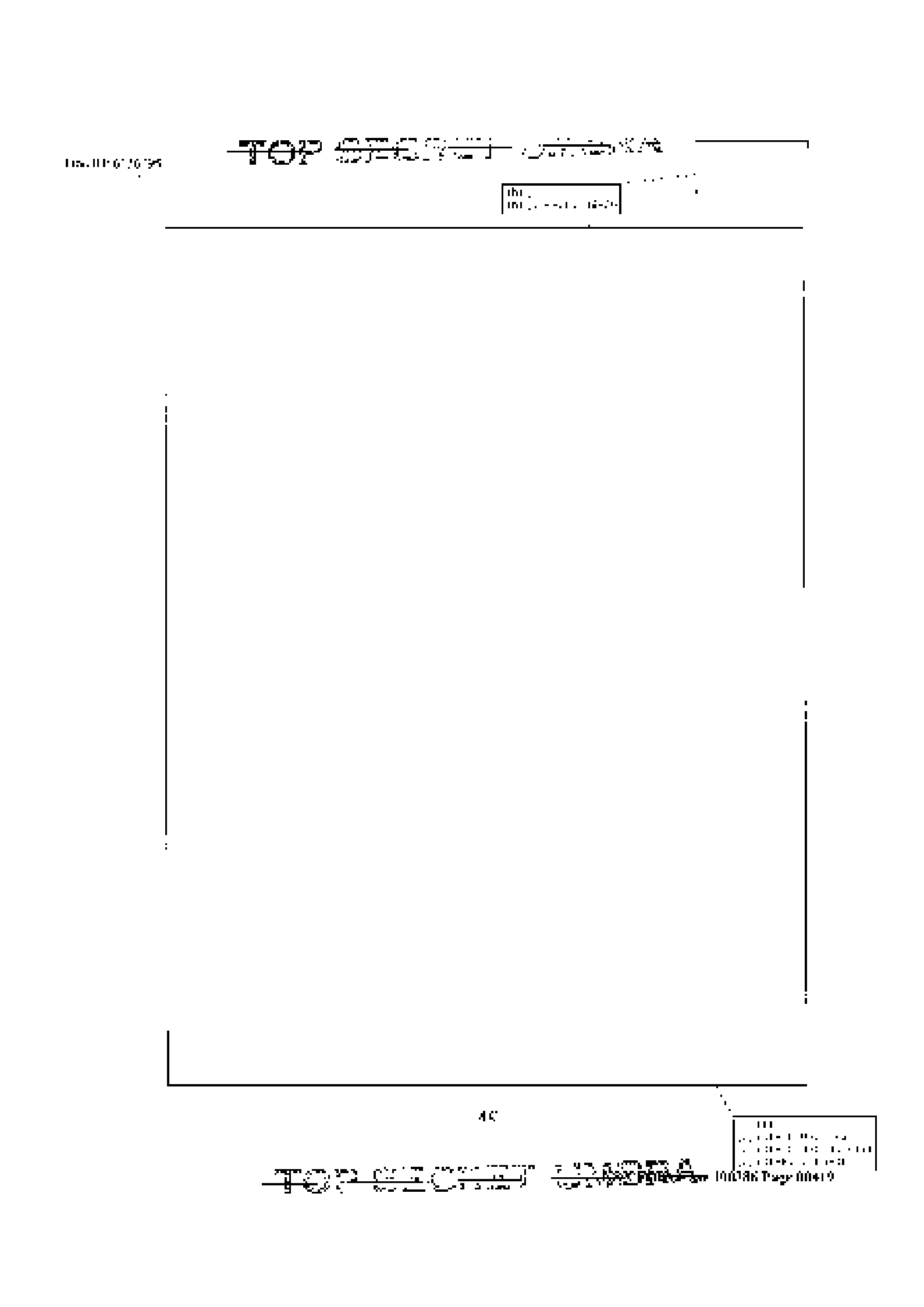
DETAILS OF UKUSA
DIVISION OF EFFORT ~~(C)~~

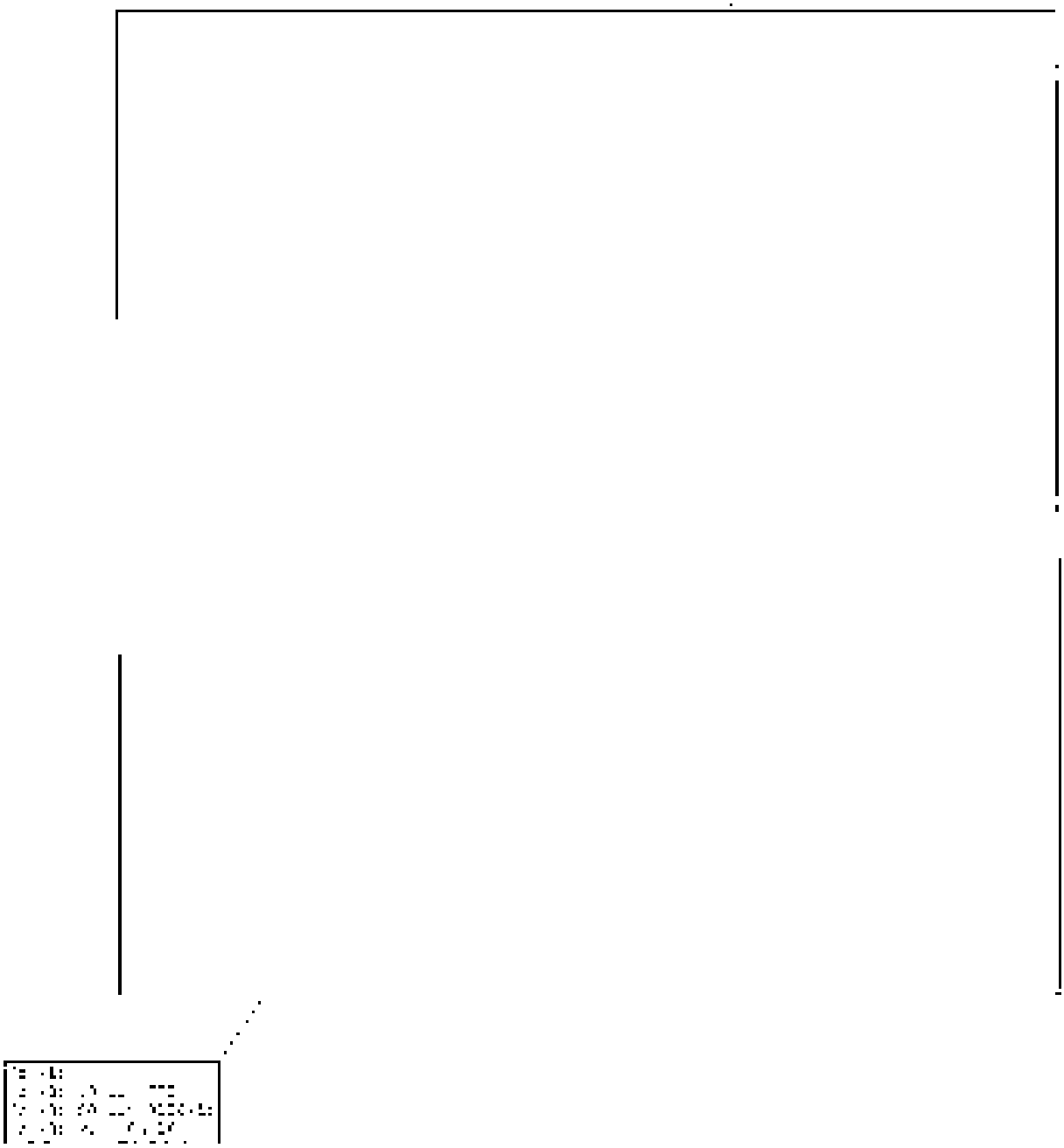
APPENDED DOCUMENTS
[illegible]



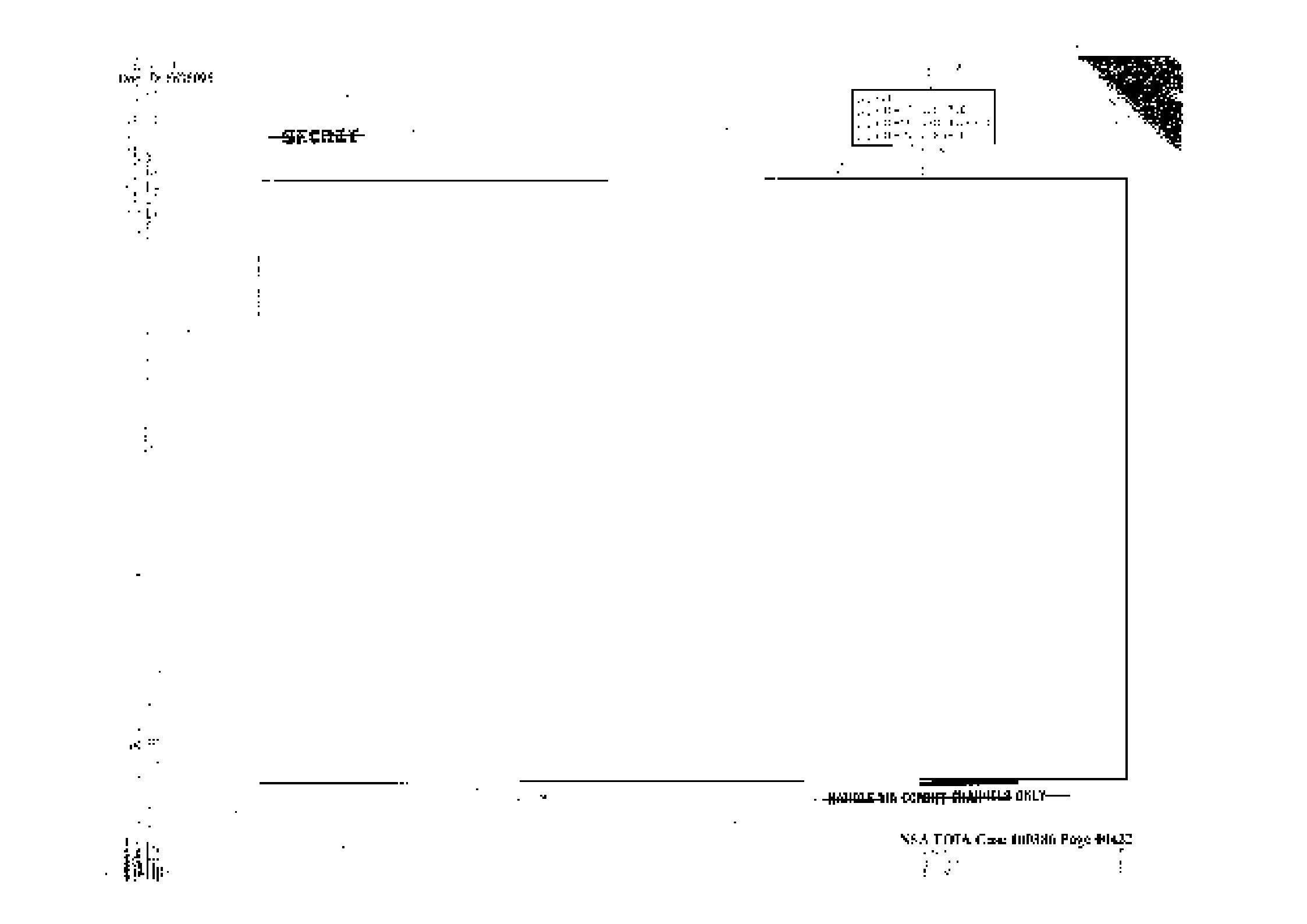
[illegible]

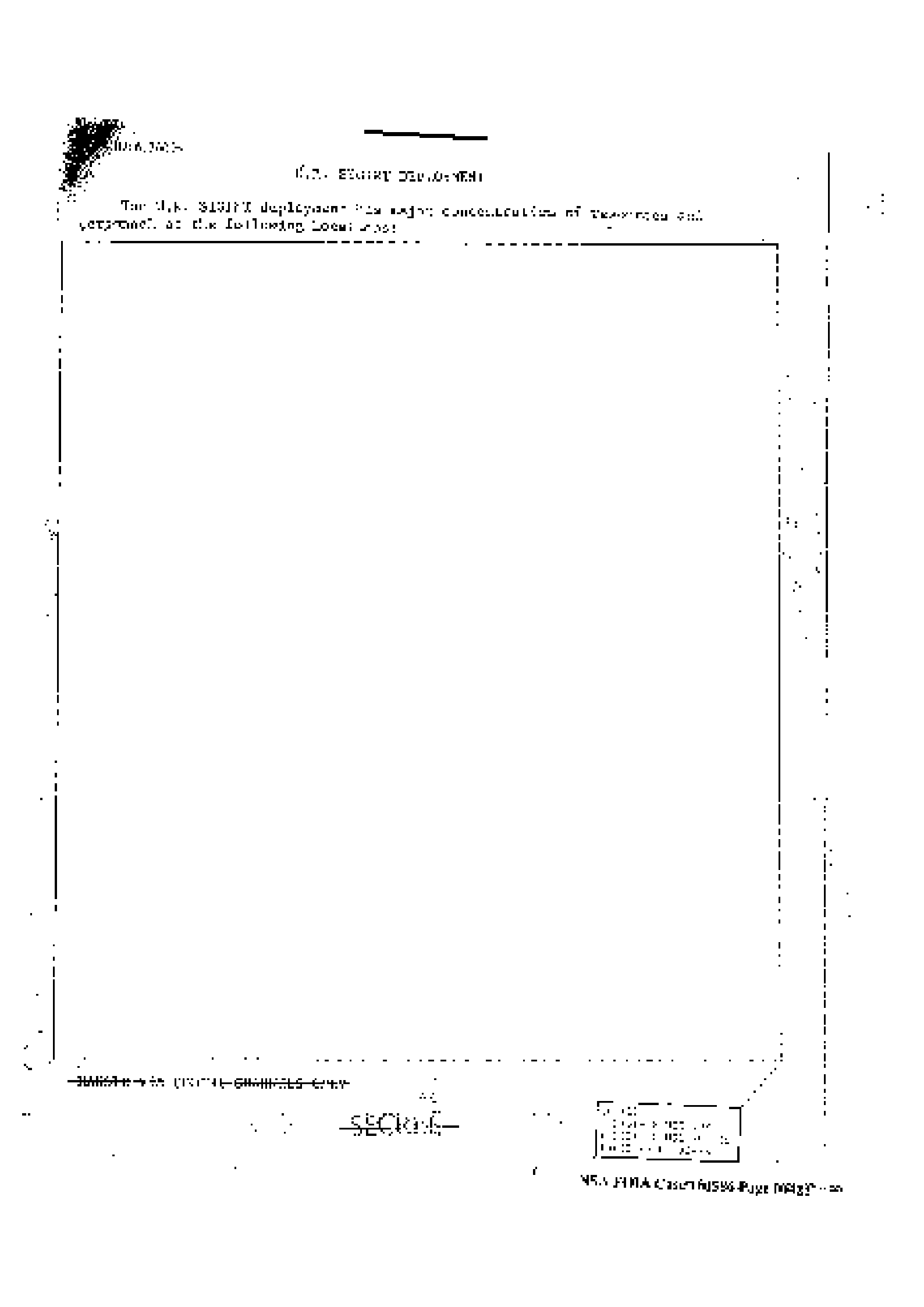






ANNEX I





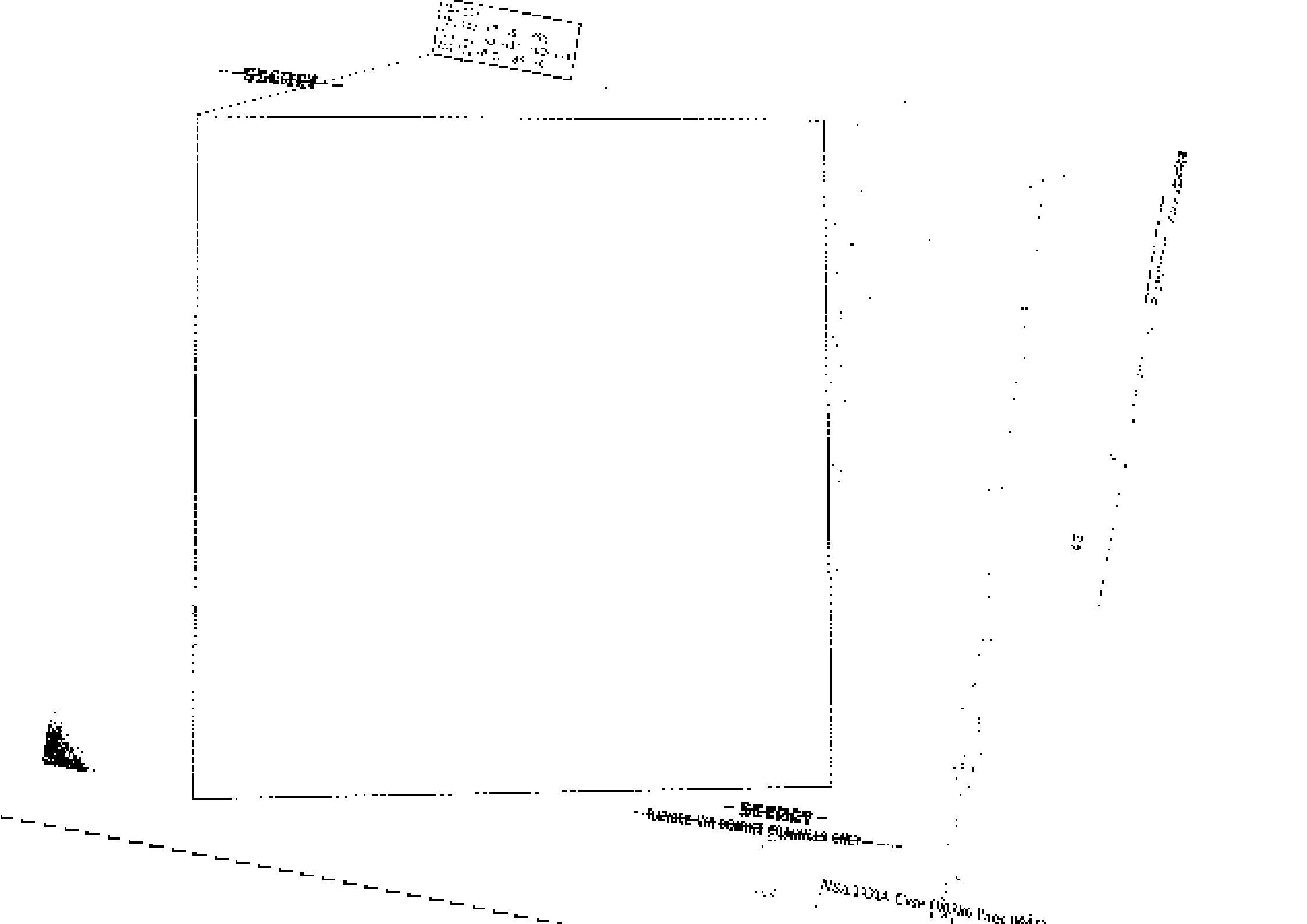
[redacted]

ANNEX B

[redacted]

[redacted]

[redacted]



"R" Rockwell Form P.R. 1-04 (12-30-57) cy D423, RADCLIFF.

PRG-042

COPY #1

~~TOP SECRET~~

BRITISH-U. S. COMMUNICATION INTELLIGENCE AGREEMENT

5 March 1946

* * *
***
*

~~TOP SECRET~~

~~TOP SECRET~~

BRITISH-U. S. COMMUNICATION INTELLIGENCE AGREEMENT

5 March 1946

~~TOP SECRET~~

TOP SECRET

TOP SECRET

OUTLINE OF

BRITISH-U. S. COMMUNICATION INTELLIGENCE AGREEMENT

1. Parties to the Agreement
2. Scope of the Agreement
3. Extent of the Agreement - Products
4. Extent of the Agreement - Methods and Techniques
5. Third Parties to the Agreement
6. The Dominions
7. Channels between U. S. and British Empire Agencies
8. Dissemination and Security
9. Dissemination and Security - Commercial
10. Previous Agreements
11. Amendment and Termination of Agreement
12. Activation and Implementation of Agreement

TOP SECRET

TOP SECRET

2.

BRITISH-U. S. COMMUNICATION INTELLIGENCE AGREEMENT

1. Parties to the Agreement

The following agreement is made between the State-Army-Navy Communication Intelligence Board (STANCIB) (representing the U. S. State, Navy, and War Departments and all other U. S. Communication Intelligence[1] authorities which may function) and the London Signal Intelligence (SIGINT) Board (representing the Foreign Office, Admiralty, War Office, Air Ministry, and all other British Empire[2] Communication Intelligence authorities which may function).

2. Scope of the Agreement

The agreement governs the relations of the above-mentioned parties in Communication Intelligence matters only. However, the exchange of such collateral material as is applicable for technical purposes and is not prejudicial to national interests will be effected between the Communication Intelligence agencies in both countries.

[1]Throughout this agreement Communication Intelligence is understood to comprise all processes involved in the collection, production, and dissemination of information derived from the communications of other nations.

[2]For the purposes of this agreement British Empire is understood to mean all British territory other than the Dominions.

* To be supplied by the U.K.

3. Extent of the Agreement - Products

(a) The parties agree to the exchange of the products of the following operations relating to foreign communications:[3]

(1) collection of traffic

(2) acquisition of communication documents and equipment

(3) traffic analysis

(4) cryptanalysis

(5) decryption and translation

(6) acquisition of information regarding communication organizations, practices, procedures, and equipment.

---

[3]Throughout this agreement foreign communications are understood to mean all communications of the government or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor, and shall include [redacted] communications of a foreign country which may contain information of military, political, or economic value. Foreign country as used herein is understood to include any country, whether or not its government is recognized by the U. S. or the British Empire, excluding only the U. S., the British Commonwealth of Nations, and the British Empire.

(b) Such 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. It is the intention of each party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon.

4. Extent of the Agreement - Methods and Techniques

(a) The parties agree to the exchange of information regarding methods and techniques involved in the operations outlined in paragraph 3(a).

(b) Such exchange will be unrestricted on all work undertaken, except that upon notification of the other party information may be withheld by either party when its special interests so require. Such notification will include a description of the information being withheld, sufficient in the opinion of the withholding party, to convey its significance. It is the intention of each party to limit such exceptions to the absolute minimum.

5. Third Parties to the Agreement

Both parties will regard this agreement as precluding action with third parties[4] on any subject appertaining to Communication Intelligence except in accordance with the following understanding:

---

[4]Throughout this agreement third parties are understood to mean all individuals or authorities other than those of the United States, the British Empire, and the British Dominions.

(a) It will be contrary to this agreement to reveal its existence to any third party whatever.

(b) Each party will seek the agreement of the other to any action with third parties, and will take no such action until its advisability is agreed upon.

(c) The agreement of the other having been obtained, it will be left to the party concerned to carry out the agreed action in the most appropriate way, without obligation to disclose precisely the channels through which action is taken.

(d) Each party will ensure that the results of any such action are made available to the other.

6. The Dominions

(a) While the Dominions are not parties to this agreement, they will not be regarded as third parties.

(b) The London SIGINT Board will, however, keep the U. S. informed of any arrangements or proposed arrangements with any Dominion agencies.

(c) STANCIB will make no arrangements with any Dominion agency other than Canadian except through, or with the prior approval of, the London SIGINT Board.

(d) As regards Canada, STANCIB will complete no arrangements with any agency therein without first obtaining the views of the London SIGINT Board.

(e) It will be conditional on any Dominion agencies with whom collaboration takes place that

they abide by the terms of paragraphs 5, 8, and 9 of this agreement and to the arrangements laid down in paragraph 7.

7. Channels Between U. S. and British Empire Agencies

(a) STANCIB will make no arrangements in the sphere of Communication Intelligence with any British Empire agency except through, or with the prior approval of, the London SIGINT Board.

(b) The London SIGINT Board will make no arrangements in the sphere of Communication Intelligence with any U. S. agency except through, or with the prior approval of, STANCIB.

8. Dissemination and Security

Communication Intelligence and Secret or above technical matters connected therewith will be disseminated in accordance with identical security regulations to be drawn up and kept under review by STANCIB and the London SIGINT Board in collaboration. Within the terms of these regulations dissemination by either party will be made to U. S. recipients only as approved by STANCIB; to British Empire recipients and to Dominion recipients other than Canadian only as approved by the London SIGINT Board; to Canadian recipients only as approved by either STANCIB or the London SIGINT Board; and to third party recipients only as jointly approved by STANCIB and the London SIGINT Board.

9. Dissemination and Security - Commercial

STANCIB and the London SIGINT Board will ensure that without prior notification and consent of the other party in each instance no dissemination of information derived from Communication Intelligence sources is made to any individual or agency, governmental or otherwise, that will exploit it for commercial purposes.

10. Previous Agreements

This agreement supersedes all previous agreements between British and U. S. authorities in the Communication Intelligence field.

11. Amendment and Termination of Agreement

This agreement may be amended or terminated completely or in part at any time by mutual agreement. It may be terminated completely at any time on notice by either party, should either consider its interests best served by such action.

12. Activation and Implementation of Agreement

This agreement becomes effective by signature of duly authorized representatives of the London SIGINT Board and STANCIB. Thereafter, its implementation will be arranged between the Communication Intelligence authorities concerned, subject to the approval of the London SIGINT Board and STANCIB.

For and in behalf of the London Signal Intelligence Board:

Patrick Marr-Johnson
Colonel, British Army
General Staff

For and in behalf of the State-Army-Navy Communication Intelligence Board:

Hoyt S. Vandenberg
Lieutenant General, USC
Senior Member

5 March 1946

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

T : +33 (0)3 88 41 20 18
F : +33 (0)3 88 41 27 30
www.echr.coe.int

Ms Megan Goulding
LIBERTY
Liberty House
26-30 Strutton Ground
UK – London SW1P 2HR

GRAND CHAMBER

ECHR-LE21.7R
PMC/ji

21 February 2019

BY E-TRANSMISSION ONLY

Application nos. 58170/13, 62322/14 and 24960/15
Big Brother Watch and Others v. the United Kingdom
Application concerned: 24960/15 – 10 Human Rights Organisations and Others v. the United Kingdom

Dear Madam,

Further to my letter of 4 February 2019 informing the parties that the above case has been referred to the Grand Chamber, I write to advise you that the Grand Chamber constituted to consider this case (Rule 24 of the Rules of Court) is composed as follows:

Guido Raimondi, *President,*
Angelika Nußberger,
Robert Spano,
Vincent A. De Gaetano,
Jon Fridrik Kjølbro,
Paulo Pinto de Albuquerque,
André Potocki,
Faris Vehabović,
Iulia Antoanella Motoc,
Yonko Grozev,
Carlo Ranzoni,
Mārtiņš Mits,
Gabriele Kucsko-Stadlmayer
Marko Bošnjak,
Tim Eicke,
Darian Pavli,
Erik Wennerström, *judges,*
Işıl Karakaş,
Egidijus Kūris,
Paul Lemmens, *substitute judges.*

Written Procedure

The President of the Grand Chamber has directed that the parties shall have until **3 May 2019** to make further written submissions. You will be informed shortly of the particular issues which the Court wishes the parties to address in those submissions.

A copy of each party's memorial will be sent to the other party for information and, where appropriate, comment.

The President has also directed that the applicants in the 3 joined cases should submit a single memorial. I would therefore ask you to agree to a representative who will act as the one point of contact in these applications and to inform me as soon as possible of the details of that person.

The core bundle of documents agreed by the parties in advance of the Chamber hearing will be admitted to the Grand Chamber hearing file.

Finally, I draw your attention to the fact that your claims under Article 41 of the Convention remain as originally submitted. However, within the above-mentioned time-limit, you may amend the original claims for costs and expenses in order to take account of the proceedings before the Grand Chamber.

Oral Procedure

Any specific points on which the Court might wish to hear the parties will be sent to you at a later stage.

The President of the Grand Chamber has directed that the hearing shall take place on **10 July 2019** at **9.15 a.m.** He will meet the parties' representatives in his office on the same date at **8.45 a.m.** in order to discuss certain preliminary procedural issues. Each party shall have a maximum of thirty minutes for initial submissions to the Court and ten minutes for submissions in the second round. In both rounds the floor will be given first to the applicants' and then to the Government's representatives. The hearing should end by **11.15 a.m.** at the latest.

I would also advise you that a hearing in the case of *Centrum för rättvisa v. Sweden* (application no. 35252/08) will take place on the same date at 2.45 p.m.

Yours faithfully,

Søren Prebensen
Deputy Grand Chamber Registrar

New U.K. Law Fails European Court Standards on Mass Interception Disclosed by Snowden

by Scarlet Kim

September 27, 2018

Last week, the European Court of Human Rights issued a major judgment in three consolidated cases challenging the U.K. government's mass interception program, which was first revealed by Edward Snowden in 2013. That judgment finds notable deficiencies in the legal framework governing mass interception, rendering the program unlawful under Articles 8 and 10 of the European Convention on Human Rights (ECHR), which protect the rights to privacy and freedom of expression.

The response of the U.K. government has been to point to new surveillance legislation – the Investigatory Powers Act 2016 (IPA) – passed during the course of the proceedings, which it asserts fixes the flaws identified by the Court. David Omand, a former director of the Government Communications Headquarters (GCHQ), the U.K. signals intelligence agency, similarly dismissed the judgment on the grounds that "[i]t tells us very little new since parliament had already accepted the need to tighten up the regulation of bulk powers."

But the particular failings identified by the Court persist in the U.K.'s new surveillance framework. Those failings relate to how GCHQ (1) selects the "bearers" within fiber optic cables for interception, (2) searches communications obtained from those cables, (3) examines communications-related metadata, and (4) searches and examines information subject to journalistic privilege.

The U.K.'s Mass Interception Program

GCHQ conducts mass interception of internet traffic by tapping the undersea fiber optic cables landing in the U.K. Fiber optic cables contain fibers that carry internet traffic, and those fibers in turn carry "bearers." GCHQ has described "bearers" as being "analogous to different television channels – there are various ways of feeding multiple bearers down a single optical fibre, with the commonest being to use light of different frequencies."

GCHQ selects bearers to intercept, then directs a copy of intercepted internet traffic to buffers, which are temporary storage spaces that reportedly retain content for three days and metadata for 30 days. This information is then filtered and searched according to "selectors" and "search criteria." The U.K. government has provided email addresses and telephone numbers as common examples of "selectors," but the full scope of permissible selectors is not known. And we know even less about what can constitute "search criteria."

Intercepted information is stored in databases, which analysts can query, data-mine, or use to call up information to examine further. In September 2015, a new disclosure of Snowden documents revealed three GCHQ programs, which shed light on the ways in which the U.K. government uses the mass interception of metadata. One program is Black Hole, a metadata repository storing "email and instant messenger records, details about search engine queries, information about social media activity, logs related to hacking operations, and data on people's use of tools to browse the internet anonymously," according to The Intercept. Another program, Mutant Broth, sifts through Black Hole data related to cookies – which are stored on devices to identify and track people browsing the internet – to monitor internet use and uncover online identities. The third program cited in the disclosed material is Karma Police, which the documents say "aims to correlate every user visible to passive SIGINT with every website they visit, hence providing either (a) a web browsing profile for every visible user on the internet or (b) a user profile for every visible website on the internet."

The Court's Findings on the Mass Interception Program

1. The Violation of the Right to Privacy under Article 8

The European Court of Human Rights held that the U.K. government's mass interception program, authorized under section 8(4) of the Regulation of Investigatory Powers Act 2000 (RIPA), violated Article 8 of the ECHR in two key respects. First, the process for selecting "bearers" and filtering and searching communications lacked "safeguards…sufficiently robust to provide adequate guarantees against abuse" (§ 347). Second, the program lacked "any real safeguards" for selecting communications-related metadata for examination (§ 387).

a. "Bearers," "Selectors," and "Search Criteria"

With respect to "bearers," while the Court concluded that "the safeguards governing the[ir] selection…for interception" were not "sufficiently robust," it provided little guidance as to what those safeguards should entail (§ 347). Its only recommendation comes in its citation to a report by the Intelligence and Security Committee (ISC) of Parliament, produced in the aftermath of the Snowden revelations, which noted that neither Ministers nor Commissioners "have any significant visibility" of the selection of bearers. The ISC further recommended "retrospective review or audit" of this process. The Court agreed that, "[a]s the ISC observed, it would be desirable for the criteria for selecting the bearers to be subject to greater oversight by the Commissioner." (§ 338)

The Court's criticism of the process for filtering and searching communications using "selectors" and "search criteria" was significantly more pointed. In particular, it suggests that this process should be subject to some form of *ex ante* independent or judicial oversight.

For instance, the Court noted that the "certification by the Secretary of State," which accompanies any warrant to authorize mass interception, sets out "categories…in very general terms (for example, 'material providing intelligence on terrorism…')." The Court observed that "it would be highly desirable for the

certificate to be expressed in more specific terms" (but the ruling clarified that the specific "selectors" and "search criteria" themselves do not "necessarily need to be listed in the warrant") (§§ 340, 342).

The Court also noted with dismay that "the only independent oversight of the process of filtering and selecting intercept data for examination is the *post factum* audit by the Interception of Communications Commissioner." It concluded that, "[i]n a bulk interception regime, where the discretion to intercept is not significantly curtailed by the terms of the warrant, the safeguards applicable at the filtering and selecting for examination stage must necessarily be more robust." (§ 346)

b. Communications-Related Metadata

The Court also found unacceptable that the U.K. government's mass interception regime permits "related communications data of all intercepted communications – even internal communications [(*i.e.* communications of persons in the UK)] incidentally intercepted as a 'by-catch'" to be "searched and selected for examination without restriction." (§ 348) Notably, the Court rejected the government's assertion that "the acquisition of related communications data is necessarily less intrusive than the acquisition of content." (§ 349) The Court explained:

> "For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with…" (§ 356).

The Court found specifically unlawful the U.K. government's exemption of communications-related metadata from safeguards set out in section 16 RIPA. Those safeguards generally require that "intercepted material is read, looked at or listened to…[only] to the extent" that it is not "referable to an individual who is known to be for the time being in the British Islands." In other words, they protect the communications of persons within the U.K. from the mass interception regime, "since persons of interest to the intelligence services who are known to be in the British Islands could be subject to a targeted warrant under section 8(1) of RIPA." (§ 343)

The Court concluded that the exemption of metadata from this safeguard does not strike "a fair balance between the competing public and private interests" and should be limited only "to the extent necessary to determine whether an individual is, for the time being, in the British Islands." (§ 357)

2. The Violation of the Right to Freedom of Expression under Article 10

The Court extended and amplified its criticisms about "the lack of transparency and oversight of the criteria for searching and selecting communications for examination" in the context of journalistic communications. It noted:

> "[I]t is of particular concern that there are no [public] requirements…either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material is or may be involved. Consequently, it would appear that analysts could search and examine without restriction both the content and the related communications data of these intercepted communications." (§ 493)

The Court indicated that there should be "arrangements limiting the intelligence services' ability to search and examine such material other than where 'it is justified by an overriding requirement in the public interest.'" (§ 495) And it

suggested that there should be "sufficient safeguards relating both to the circumstances in which they may be selected intentionally for examination, and to the protection of confidentiality where they have been selected, either intentionally or otherwise." (§ 492) Unfortunately, however, the Court articulated no additional guidance in its decision, including what those safeguards might look like in practice.

The Investigatory Powers Act Fails to Fix the Problems

1. "Bearers," "Selectors," and "Search Criteria"

Before delving into the details of whether the IPA has anything to say about the authorization and oversight of "bearers," "selectors," and "search criteria" (spoiler alert, it doesn't), it's worth stepping back and considering how these processes are set out more generally within the U.K.'s new surveillance framework.

The U.K. government has coined the phrase "double lock" to describe its new authorization process for approving certain surveillance powers, including mass interception. But the supposed "double lock" is really just a single lock and that lock is not especially secure.

As with the prior mass interception regime under RIPA, the IPA preserves the power of the Secretary of State to issue warrants. From a human rights perspective, the Secretary of State's involvement is not a lock because, as a member of the executive branch, the Secretary of State lacks the necessary independence.

And while the IPA permits Judicial Commissioners to "approve" this decision, there remain significant questions about the scope of scrutiny they may exercise in reviewing warrants. For example, section 140 of the IPA provides that Judicial Commissioners must "review the Secretary of State's *conclusions*" on whether a warrant is necessary and proportionate and "apply the same principles as would be

applied by a court on an application for judicial review." Debate continues to swirl around what the "judicial review" standard will mean in practice, especially in the context of bulk warrants.

As for oversight, the IPA provides for an Investigatory Powers Commissioner, who has replaced the prior Interception of Communications Commissioner, the Chief Surveillance Commissioner, and the Intelligence Services Commissioner. The consolidation of oversight under a single Commissioner is a welcome improvement. But what that oversight will look like in practice remains subject to some speculation. The IPA speaks in broad, sweeping terms, providing that the new Commissioner "must keep under review" the various surveillance powers authorized by the IPA (section 229).

So at least with respect to the face of the IPA itself, it has absolutely nothing to say about whether there should be *ex ante* authorization or *ex post* oversight of "bearers," "selectors," and "search criteria." And what the above digression reveals is that the very structure of the new authorization process raises serious questions as to how it would function as a vehicle for reviewing issues at the granularity of "selectors" and "search criteria." Whether the selection of "bearers" becomes a subject of the oversight activities of the new Investigatory Powers Commissioner is a development we can only wait to observe.

2. Communications-Related Metadata

The IPA treats communications-related metadata similarly to RIPA, with one exception. Like RIPA, it generally adds another layer of safeguards for the communications content of persons known to be in the U.K. but does not extend those protections to the metadata attached to such communications. The perpetuation of this distinction is even more troubling considering that the IPA, unlike RIPA, provides that certain content, in and of itself, can be extricated from intercepted communications and treated as metadata (section 137(5) IPA).

The IPA does provide that the selection for examination of metadata – as with content – now must be for a stated operational purpose (section 152 IPA). But those purposes are exceedingly broad and simply those "specified in a list maintained by the heads of the intelligence services…as purposes which they consider are operational purposes for which intercepted content or secondary data…may be selected for examination" (section 142(4) IPA). In any event, this safeguard falls far short of what the Court indicates is necessary, which is to subject the communications content and metadata of persons in the U.K. to the same protections except for when examining metadata for the purpose of "determin[ing] whether an individual is, for the time being, in the British Islands." (§ 357)

3. Confidential Journalistic Material

The IPA contains a single safeguard related to "confidential journalistic material" in the section devoted to mass interception – that where such a communication "is retained, following its examination, for purposes other than [its] destruction," the agency "must inform the Investigatory Powers Commissioner" (section 154 IPA). The Interception of Communications Code of Practice provides some additional guidance. Where an analyst intends to select for examination confidential journalistic material (or content "in order to identify or confirm a source of journalistic information"), "he or she must notify a senior official" outside of the agency who "may only approve…if he or she considers that the Agency has arrangements in place for the handling, retention, use and destruction" of such communications (paras. 9.84, 9.86).

Neither of these safeguards satisfy the requirements set out in the Court's ruling. First, the Court indicates that such communications should be selected for examination only where "justified by an overriding requirement in the public interest," and no such assessment is built into the safeguards described above. Second, the Court provides that there should be safeguards both for "the circumstances in which [confidential journalistic material] may be selected intentionally for examination, and to the protection of confidentiality where they have been selected." The safeguards described above do not address the latter;

while the Code of Practice "handling" safeguard could potentially encompass this point, it does not appear sufficiently clear. Moreover, it remains questionable whether authorization by a "senior official" (who would appear to be someone designated by the Secretary of State for that purpose) is appropriate, as opposed to an independent authority.

Intelligence Sharing and the IPA

The Court's judgment did not just address the U.K. government's mass interception program but also its access to information collected by foreign intelligence agencies, including the U.S. National Security Agency. That part of the judgment explicitly articulated, for the first time, that where a government obtains information through such access, the interference with the right to privacy is equivalent to obtaining that information through direct surveillance.

The Court held that such a regime, like any direct surveillance regime, must therefore "be 'in accordance with the law'…, proportionate to the legitimate aim pursued, and [provide] adequate and effective safeguards against abuse." It added that "[i]n particular, the procedures for supervising the ordering and implementation of the measures in question must be such as to keep the 'interference' to what is 'necessary in a democratic society.'" (§ 422)

Unfortunately, the Court's judgment sanctions the U.K.'s intelligence-sharing regime, despite the fact that it falters under these very principles, both under RIPA and the IPA. RIPA had nothing to say about intelligence sharing. But the Court nevertheless found the "statutory framework" governing this activity sufficient because the U.K. government had disclosed a "note" during the domestic proceedings purporting to lay out the rules governing intelligence sharing. Never mind that the note consisted of 2 pages, with no heading, no author, and no indication of whether it represented an actual policy, part of a policy, a summary of a policy, or a summary of submissions made by the U.K. government during a closed hearing on the issue.

The Court also made much of the fact that the note was substantially reproduced in the Interception Communications Code of Practice. But the language of the note and Code of Practice remain woefully inadequate. Notably, both speak of the U.K. government making a "request" for "unanalyzed intercepted communications content (and secondary data)." The concept of "request" is an antiquated one that fails to address the manner in which intelligence agencies swap information in the digital age, for example, by offering direct and unfettered access to raw data intercepted in bulk or databases of material collected in bulk. No "request" is required in such circumstances.

The IPA suffers from the same deficiencies and more. Only one provision explicitly addresses the U.K. government's access to foreign intelligence information. That provision (section 9 IPA) provides that the U.K. may not "request" foreign authorities to "carry out the interception of communications sent by, or intended for" a person in the U.K. unless an appropriate warrant has been issued. Thus, this provision again focuses on "requests" by the U.K. to foreign authorities. It is also limited to the interception of communications related to a person in the U.K.

Finally, the Court, perhaps because of its basic misunderstanding of the nature of modern intelligence sharing, essentially sanctions aspects of the U.K.'s mass interception framework as it applies to intelligence sharing, even as it found that very framework unlawful. It notes that "those requirements which relate to… storage, examination, use, onward dissemination, erasure and destruction" in the direct surveillance context must also "be present" in the intelligence sharing regime (§ 423). And yet, it found no need to extend its concerns about how the U.K. government filters and searches bulk intercept material to how it might similarly filter and search databases of bulk intercept material maintained under a foreign government's mass surveillance program.

*****

In the coming months, the U.K. government is likely to continue to trot out the passage of the IPA as evidence that its mass interception program now rights the failings identified by the Court. As discussed above, that claim falters against a close reading of the IPA.

The U.K. is far from the only country to operate a mass interception program. The U.S. operates analogous programs, as do several Council of Europe members. The Court's judgment provides a new and important guidepost for evaluating these programs as well.

NSA whistleblower Edward Snowden speaks via videoconference during the 2014 SXSW Music, Film + Interactive Festival in Austin, Texas. (Photo by Michael Buckner/Getty Images for SXSW)

DATE 7/22/2015

Note

OPERATIONS DIRECTORATE REGISTRY (DOR)

ACTION	INFORMATION	NUMBER	ORIGINATOR
SUBJECT: Release of NRO/NSA Exchange Agreement		DATE RECEIVED: Oct 12/3/54	
		EXT. CONTROL: NSA-015-94	
ACTION TO: DoV	COPIES TO: A, B, C, D, Z	SUSPENSE: 15 Feb 94	

DDO ACTION REQUIRED

SIGNATURE	RETURN	DISPATCH	INITIALS

DOC

ATCH

ADDN DOC

NOTE: This slip must be appended to the completed action and returned to the DOR for records logging and forwarding.

[redacted]

DDO

SECRET

UNITED STATES GOVERNMENT

memorandum

DATE 15 January 1998 REPLY TO ATTN OF P52-01-98

SUBJECT Review of USUSA Exchange Agreement (U)

TO DISTRIBUTION

1. (S-CCO/NF) Request your support in reviewing the USUSA Exchange Agreement. This information will satisfy the foreign reviews and assist currently underway with Congressional, DoD, and GAO staffs, in addition to providing a comprehensive study of current exchange policies with [redacted].

2. (S-CCO/NF) In Nov 1993, DIA initiated an operational review of the UKUSA Exchange Agreement to include a list of what is now currently exchanged with the British, what we should not exchange in the future, and new things that should be exchanged in the future. Attached is a copy of the memo asking each DDO Group to review the agreement (see Attachment A).

3. (S-CCO/NF) In Dec 1993, the Country Desk Officer (CDO) for the United Kingdom met with DIA, DOE, and DDI staff elements to discuss the aforementioned effort and explain that NSA was trying to satisfy external audits and reviews of UKUSA as well. Everyone agreed that a "1" Agency review would be appropriate in light of the cooperative involved in providing a "1" glimpse of the exchange. By combining reports, we could eliminate duplication and provide a more comprehensive paper that would be easily updated on a routine basis.

4. (S-CCO/NF) Attachment B provides a format for presenting the information, detailing 7 categories: (1) by country, and (2) by topic (ref Attachment C for list of topics). For each country and topic, identify exactly what is exchanged in terms of raw traffic, product and technical reports, [redacted] hardware, software. A similar study was prepared by DDO in 1987 to satisfy a DCI directed study of the [redacted] relationship. If each group can find their submission to this study, it would make an excellent basis for the working level's input (see Attachment B).

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

NSA NOTA Case 100886 Page 00204

Date: 6/3/85

~~SECRET~~ N-89-019-04

[redacted]

1. S. ~~(S-CCO/REL~~ Where possible, request copies of any Memorandums of Understanding or Divisions of Effort between NSA and [redacted] will be provided in support of this exchange. [redacted] Compartmented exchanges should be included in an Annex and referenced as such in its associated country or topic (e.g., [redacted]). Please provide information on an ASCII format so that data can be transferred into a spreadsheet format.

2. ~~(C-CCO/REL~~ We anticipate periodic meetings to discuss the status as necessary. Given the multiple requirements to respond to Congressional, DoD, and OSD queries, we need your input by 14 Feb 1986. Please direct any questions on this request to [redacted] or [redacted] on 688-5485.

[redacted]

JOHN M. DINGS
Director of Foreign Relations

Encl:
a/a

DISTRIBUTION:

DCC
DCI
DCI

CIA: DDI
[redacted]
NSA
ADCI
DDCI
DDCI/C&I
DDCI/E
DDCI/S
DDCI/PA
DDCI/A
IC

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

NSA FOIA Case 80080 Page 00005

[illegible]

ATTACHMENT A

~~SECRET~~

UNITED STATES GOVERNMENT

memorandum

DATE: 19 November 1990

REPLY TO ATTN OF: DCAM-142-04

SUBJECT: [illegible] Exchange Agreement ACTION REQUIRED

TO: [illegible]

1. ~~(S-REL USA)~~ The CIO has marked the ESI sheets to be used for the US-UK Exchange Agreement. Please check all the entries carefully for additional data in terms of each new agreement and what it is like to see. It would be extremely economical to [illegible] We have decided to break the [illegible] of the following parts:

- Part I: List of additional double check entries that are not for the best of your knowledge; exchanged with the UK body.

- Part II: [illegible] This part will check [illegible] that services and agents [illegible] may well need to be altered or declassed [illegible] in the near future (1 - 3 years at least) given certain assumptions about developments affecting US-UK relations. Include an "expert" [illegible] of the exact item and 2-3 sentences describing the assumption leading to an alteration or denial of the currently exchangeable [illegible] items should be made in ASCII format on a floppy disk.

- Part III: List those new things that should be exchanged with the UK in the future. Include an "expert" [illegible] for each item and 2-3 sentences describing the assumption leading to possible exchange. Inputs should be made in ASCII format on a floppy disk.

2. [illegible] Time Timeline:

- By Mid-November - send copy of task to each of the Corps Chiefs, and Chiefs [illegible].

HANDLE VIA COMINT CHANNELS ONLY

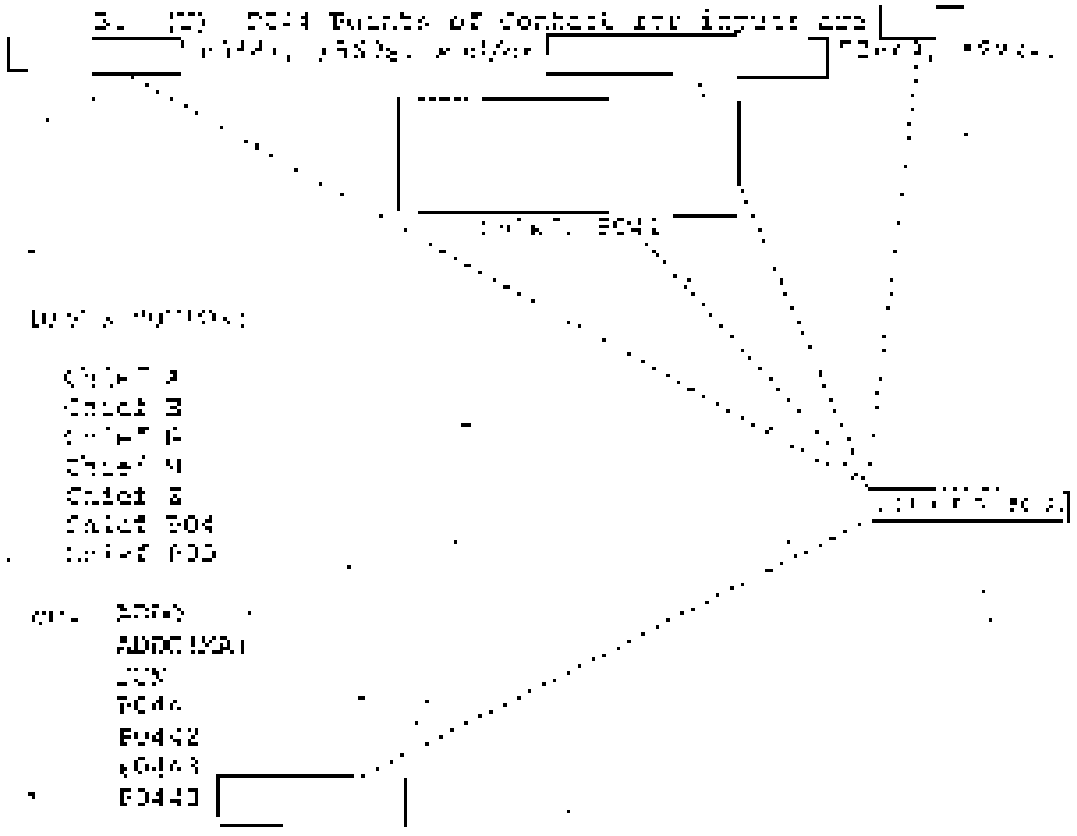
~~SECRET~~ ~~NOFORN~~

[illegible]

DSA FOIA Case [illegible] Page 01306

~~SECRET~~

- By 15 December -- meet with each of the Group Chiefs for 15 minutes to clarify and answer questions.
- By 15 January 1999 -- give assignments. All inputs to DCI/C for integration and preparation
- By 30 January 1999 -- DCI/C publishes final report for very restricted distribution.



~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~ ~~NOFORN~~

COUNTRY/TOPIC:

NSA INTELLIGENCE EXCHANGE WITH GCHQ

CURRENT | *NEAR FUTURE - NEXT YEAR 2000*

TYPE OF AGREEMENT	WHAT WE RECEIVE	WHAT WE PROVIDE	WHAT WE DO NOT PROVIDE (include FOCs & rationale)	WHAT WE SHOULD PROVIDE	WHAT WE SHOULD NOT PROVIDE (include FOCs & rationale)

[redacted]

[redacted] NSC-2015-04

[redacted]

ATTACHMENT C

US Foreign Intelligence
Requirements Categories and Priorities

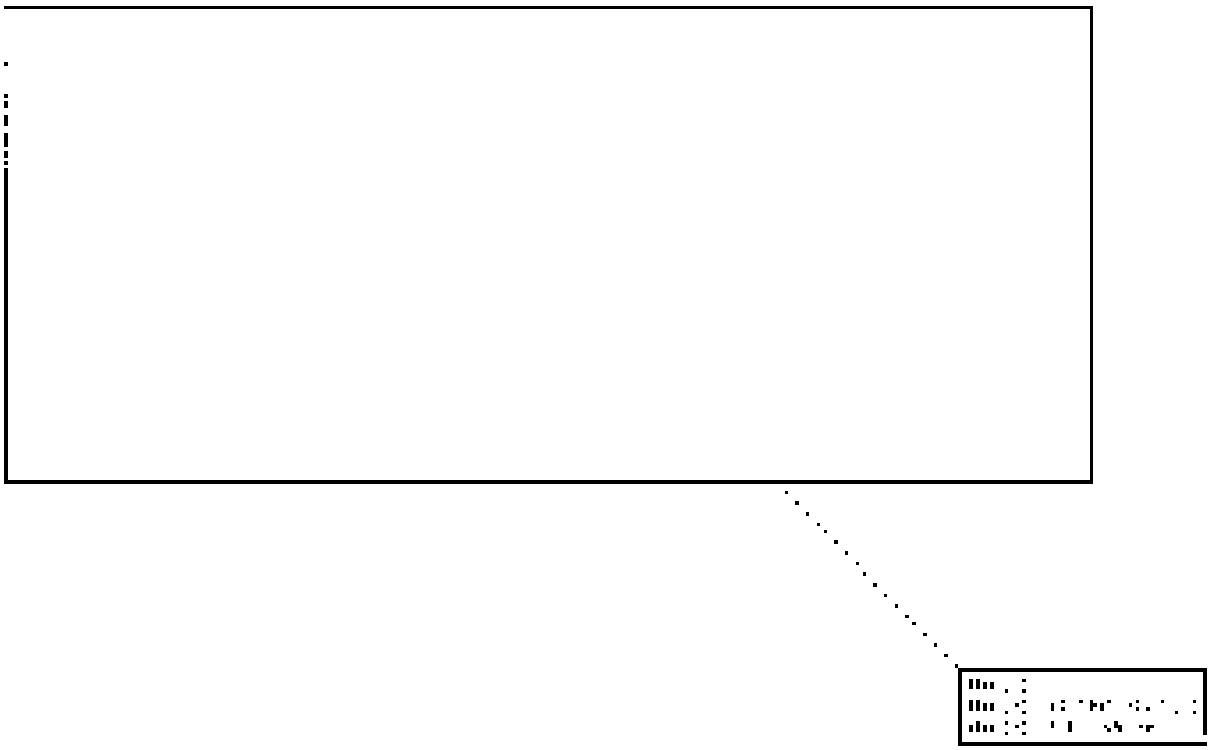
[redacted] TOPICS

[redacted]

[redacted]

[redacted]

[redacted]



NSA STAFF PROCESSING FOI # 61269 #

DIR

DEPDIR, DDP

SUBJECT: DIR Desk Note to AUDC for 8 PM Tonight-President Clinton Meeting (TS)

ACTION: [ ] APPROVAL [X] SIGNATURE [ ] INFORMATION

EXECSEC SUSPENSE:

ACTION OFFICER:

ACTION OFFICER'S PHONE:

INFO ADDEES: DDI, DDO, DDT, DIO, DIR, NA, VOF, ExReg

SUMMARY:

(TOUO) The attached note is at the request of the DIR for background information on the U.S./UK Cryptologic relationship to be forwarded to President Clinton in advance of a 21 May 97 meeting with UK Prime Minister Tony Blair.

Ben Tucker Dan Brown

DI Gardiner Report

This correspondence may be downgraded to: AUDC upon removal of the enclosure(s)

CLASSIFICATION/CONTROL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
NE					

DESIGNATOR: CDO, ITK

ORG: VOF

DATE PROCESSED: 5/14/97

Derived From: NSA/CSSM 123-2; 85Sep0...

Declassify On: OADR; 85Sep01

Page 00208

Doc ID: [illegible]

~~TOP SECRET~~

DIRECTOR

[illegible] May 1997

TO: [illegible]

SUBJ: Background for President Clinton Meeting with PM Blair (U)

(S) The Director of GCHQ, David Omand, will be briefing UK Prime Minister Tony Blair on the FISCX cryptology relationship in preparation for the upcoming session between Blair and President Clinton. The two leaders are scheduled to meet on 29 May in The Hague after the NATO summit. Would you please forward background for the President's session with the Prime Minister.

KENNETH A. MINIHAN
Lieutenant General, USAF

cc: [illegible]

[illegible]

~~TOP SECRET~~

U.S. CRYPTOLOGIC PARTNERSHIP WITH THE UNITED KINGDOM

Background (U)

(~~TS//SI~~) The U.S.-U.K. Cryptologic relationship is the oldest and most productive of NSA's foreign partnerships. It is based on a formal "UKUSA Agreement," which was signed in 1946, and includes numerous supporting agreements signed over the years with NSA's counterpart, the Government Communications Headquarters (GCHQ). This agreement is the basis for comprehensive cooperation on SIGINT and to a lesser extent, INFOSEC activities. The U.S.-U.K. cryptologic partnership will continue to be broad and deep well into the 21st Century.

Key Elements of Cryptologic Relations (U)

(~~TS//SI~~) Under the UKUSA Agreement, each side agrees to share all SIGINT product information, the exchange is unrestricted except for those products specifically excluded (e.g., U.S. ONLY or forwarded at the request of the originator).

(~~TS//SI~~) NSA's and GCHQ's intelligence priorities are largely convergent and GCHQ's SIGINT collection and processing capabilities often complement our own. Cooperation [redacted]

They have agreed to continue this partnership into the future and are currently making arrangements with the government to do so. GCHQ also has a number of advanced collection, processing, and analysis facilities. Some GCHQ [redacted] exist solely to satisfy NSA tasking. NSA and GCHQ jointly address each of these to reduce duplication and maximize coverage. Through joint assessments, despite the caveats:

(~~TS//SI~~) The cryptomathematics exchange with GCHQ is at the heart of our INFOSEC relationship. GCHQ is NSA's only peer in the field of cryptomathematics and virtually all major advances within the field of cryptography have occurred as a result of communal sharing. We enjoy a mutually beneficial exchange at the highest technical level on the design and evaluation of cryptologic systems. As NSA supports U.S. Government efforts towards achieving a secure global information infrastructure, GCHQ stands as our most influential foreign partner to advance INFOSEC policies in international fora.

~~Handle Via COMINT Channels Only~~
~~TOP SECRET~~

[redacted]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	Criminal No. 86-
JONATHAN JAY POLLARD,	)	
defendant.	)	
	)	

DECLARATION OF THE SECRETARY OF DEFENSE

CASPAR W. WEINBERGER HEREBY DECLARES AND SAYS:

1. (U) I have been the Secretary of Defense and the c executive officer of the Department of Defense (DOD), executive department of the United States, 10 U.S.C. 1 20 January 1981. As Secretary of Defense, I have autho direction and control over the DOD, 10 U.S.C. 133(b), and a member of the National Security Council.

2. (U) As Secretary of Defense, I possess original classification authority for TOP SECRET information, Sensitive Compartmented Information (SCI). SCI is in which derives from sources or methods which are espec vulnerable to unauthorized disclosures. That vulnerab

[redacted]

[redacted]

gion from particularly fragile acquisition methodology, from sources especially susceptible to counter measures or deception techniques or even from danger to human life if the substantive information obtained is exposed. The fact that I possess this classification authority means that I am authorized to determine the significance and the proper classification of national security information, including the SECRET, SENSITIVE COMPARTMENTED INFORMATION (SCI), on behalf of the United States. The information I have prepared for the Court is submitted based upon my personal review of relevant information and my discussions with personnel who are knowledgeable about the data described herein.

3. (S) The information in this declaration is submitted for use by the Court as it is in determining an appropriate sentence for the defendant, Jonathan Jay Pollard. It is my purpose to explain the nature and significance of the defendant's actions as I perceive them to have affected the security of the United States. I have detailed a considerable quantity of highly sensitive information, and therefore request that the Court review it in document and believe it prior to and have in the hands of the Court immediately upon completion of review. I also request that it not be [illegible] or reviewed by [illegible] unless it is necessary as a matter of law to do so, and then only after [illegible]

[redacted]

[redacted]

access is ascertained. Should the document again be required by the Court, or by any court with jurisdiction over this case, it will immediately be made available. I have directed that this document be retained by the Director of Naval Intelligence who will be responsible for its safekeeping and further delivery to the Court as required.

4. (U) I believe it is necessary to understand the purpose of intelligence acquisition before one can comprehend the significance of its loss. There are two primary reasons for gathering and analyzing intelligence information. The first, and most important in my view, is to gain the information required to direct U.S. resources as necessary to counter threats of external aggression. The second reason is to obtain the information necessary to scientifically and effectively direct the foreign policy of the United States. It necessarily follows that inappropriate disclosure of properly classified intelligence information intended to serve these purposes can be used to frustrate both the defensive and foreign policy goals of the United States, regardless of its recipient.

a. The ability to gain information disclosure of a hostile foreign power can be used to produce counter measures which not only [illegible] but also permit the more efficient and effective utilization of resources in pursuit of

[redacted]

[redacted]

U.S. interests.

b. Unauthorized disclosures to friendly powers may cause as great a harm to the national security as to hostile powers because, once the information is removed from secure control systems, there is no enforceable requirement nor any incentive to provide effective controls for its safekeeping. Moreover, it is more probable than not that the information will be used for unintended purposes. Finally, such disclosures will tend to expose a larger picture of U.S. capabilities and knowledge, or lack thereof, than would be in the U.S. interest to reveal to another power, even to a friendly one.

5. (U) In this case, the Government has omitted proving by testimonial contents or individually tape quantity of classified information. At the outset I must state that the defendant's unlawful disclosure did expose the limits of any official exchange of intelligence information with Israel, and being true, the damage to national security can scarcely be measured the information was given over. Finally, I would point out the fact all the information passed by the defendant, as to Israeli officials unfortunately, the victims of these crimes know it. have been passed to it so great as secret that. Moreover, the Government admits in a very passed to the Israeli handlers a

[redacted]

[redacted]

quantity of documents great enough to occupy a space six feet by six feet by ten feet. I have chosen to present in these pages the data I consider significant. In the first part I have detailed the categories of information compromised and given brief but specific examples of actual documents passed. In the second part I explain the harm I perceive to have occurred, again with specific examples. In the third part I encapsulate the overall significance of the defendant's activities.

PART ONE

CATEGORIES OF INFORMATION DISCLOSED

[redacted]

Copy [illegible] of [illegible] copies
Page [illegible] of [illegible] pages

[redacted]

PART TWO
DAMAGE TO THE NATIONAL SECURITY

14. ([redacted]) As noted previously, the breadth of the disclosures made by the defendant was incredibly large. Accordingly, the damage to U.S. national security interests resulting from those activities is similarly broad. I will detail herein, the more pertinent aspects of damage to U.S. national security as I perceive them:

a. Damage to Intelligence Sharing Agreements.

Since the activities of the defendant impact directly on U.S. intelligence activities, it is appropriate to begin with intelligence. It should be obvious that the United States has neither the opportunity nor the resources to unilaterally collect all the intelligence information we require. We compensate with a variety of intelligence sharing agreements with other nations of the world. In some of these arrangements there is virtually a full partnership which stems from recognition of common and indelible interests. Most, however, are fashioned on a quid pro quo basis. For example, the United States agrees to share with an ally certain types of intelligence information in exchange for desired information or other valuable assistance. Further, once such agreements are entered into, decisions to disclose particular classified documents or items of intelligence information are made by high level officials after a careful evaluation of the costs of

[redacted]

[redacted]

disclosure to our national security versus the benefits expected to be obtained if disclosure is approved. In some instances, especially sensitive intelligence information that is supplied by or ally or treaty because the ally agrees to furnish equally sensitive information vital to U.S. security interests.

[redacted]

[redacted]

disclosure is vitally important for U.S. interests because all interests must be balanced against one another. For example, the requirement to protect sources and methods of information acquisition, as well as the requirement to protect the substantive information received, must conform with the recipient's "need" for that information and the expectation of benefit for the United States. This usually means that substantive information is redacted from the original document containing the information prior to disclosure. The result is

[redacted]

Page 4 of 4 Pages
Page 29 of 45 Pages

[redacted]

[redacted]

To the best of my knowledge, not one of the pertinent documents provided that was authorized for official release to Israel in unredacted form.

15. [redacted] The motions of the defendant have specifically sought substantive intelligence information be provided to the Israelis, as well as the sources of that information, by placing it outside of a U.S. controlled security environment.

The United States, and virtually all of those who cooperate with us by sharing intelligence, have developed a system to protect any classified information which depends on the reliability of individuals for its effectiveness. It is also a system which varies its requirements for protection with the sensitivity of the information at stake. All classified material is required to be placed in proper storage, appropriate to its classification level, and all personnel who have custody are responsible for ensuring that proper procedures for protecting it are followed. The system necessarily depends on the integrity and reliability of the individual. So that as an individual is entrusted with more sensitive classified material as his seniority, or the perceived nature of his personal interest, will customarily increase. It is when an individual violates a security or classified trust for

[redacted]

[redacted]

which he is not responsible that safekeeping is jeopardized. In such an instance, there is no real incentive to adequately protect such information. One example of an occasion when this happens in the normal course of business is the necessary use or courier to carry highly sensitive information from one location to another. The defendant temporarily acted as such a courier, and it was his abuse of U.S. system, a system necessarily dependent on the integrity of the individual, which permitted his espionage activities to occur. Moreover, in a situation such as this one, there is every incentive to use the acquired information in a person's self interest. Examples of my reasoning follow:

[redacted]

[redacted]

PART THREE
THE SIGNIFICANCE OF THESE DISCLOSURES

21. ([redacted]) HARM TO U.S. FOREIGN POLICY:

In my opinion, the defendant's unlawful disclosures to the government of Israel have harmed U.S. foreign policy. My conclusions flow directly from the information I have discussed previously.

[redacted]

22. [redacted] COMPROMISED SOURCES AND METHODS.

I will not repeat the difficulties in reacquiring damaged sources of intelligence acquisition which have been compromised

Copy [illegible] of [illegible]
Page 4 of [illegible] Pages

[redacted]

[redacted]

23. [redacted] RISK TO U.S. PERSONNEL:

Finally, the United States must expect some amount of risk to accrue directly to U.S. personnel from the defendant's activities.

[redacted] concomitant risk with which I, as Secretary of Defense, am particularly concerned, is that U.S. combat forces, wherever they are deployed in the world, would be unacceptably endangered through successful exploitation of this data.

24. [redacted] I have provided the foregoing statement to provide

[redacted]

[redacted]

my views of the significant harm caused to national security by the defendant and as an aid to the Court. The data provided represents my opinions and conclusions stemming from my review of the data compromised, as well as from information obtained by me in my capacity as Secretary of Defense and as a member of the National Security Council. The defendant has substantially harmed the United States, and in my view, his crimes demand severe punishment. Because it may not be clear to the court that the defendant's activities have caused damage of the magnitude described, I felt it necessary to provide an impartial analysis to the Court so that an appropriate sentence could be fashioned. My foregoing comments will, I hope, dispel any presumption that disclosures of an ally are insignificant; to the contrary, substantial and irreparable damage has been done to this nation. Punishment, of course, must be appropriate to the crime, and in my opinion, no crime is more deserving of severe punishment than conducting espionage activities against one's own country. This is especially true when the individual may have voluntarily assumed the responsibility of protecting the nation's secrets. The defendant, of course, had full knowledge and understanding of the area of the information unlawfully disclosed. To demonstrate that knowledge, I have attached copies of non-disclosure agreements which he voluntarily executed. Should the Court require further

[redacted]

[redacted]

information or explanation of anything contained herein, you may provide the secret of this document with your requirements and I will respond to them.

Under penalties of perjury, I hereby declare the foregoing statements to be true and correct to the best of my knowledge information and belief.

DATED this_____ _____day of _____1984.

Caspar W. Weinberger

Copy 4 of 9 Copies.
Page 46 of 49 Pages.

[redacted]

[redacted]

GLOSSARY

1. TOP SECRET (TS): Information which if inappropriately disclosed would cause exceptionally grave damage to the national security of the United States.

2. SECRET (S): Information which if inappropriately disclosed would cause serious damage to the national security of the United States.

3. CONFIDENTIAL (C): Information which if inappropriately disclosed would cause damage to the national security of the United States.

[redacted]

8. TOP SECRET CODEWORD (TSC): Top Secret information derived from intelligence sources and methods. [redacted]

9. SECRET CODEWORD (SC): Secret information derived from intelligence sources and methods. [redacted]

(U)

~~TOP SECRET UMBRA~~

S E C R E T

AN ASSESSMENT OF THE UKUSA RELATIONSHIP: WHERE WE GO FROM HERE

(S-CCO) The UKUSA relationship has been of incalculable value to NSA and cannot be abandoned.

This paper is an honest effort by [redacted] to describe the strengths and weaknesses of the UKUSA relationship so that NSA might better be able to make hard decisions about the future of the relationship.

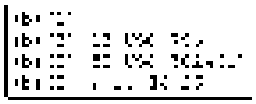
(S-CCO) There is no doubt that UKUSA places NSA much [redacted] to document a few important contributions we must include:

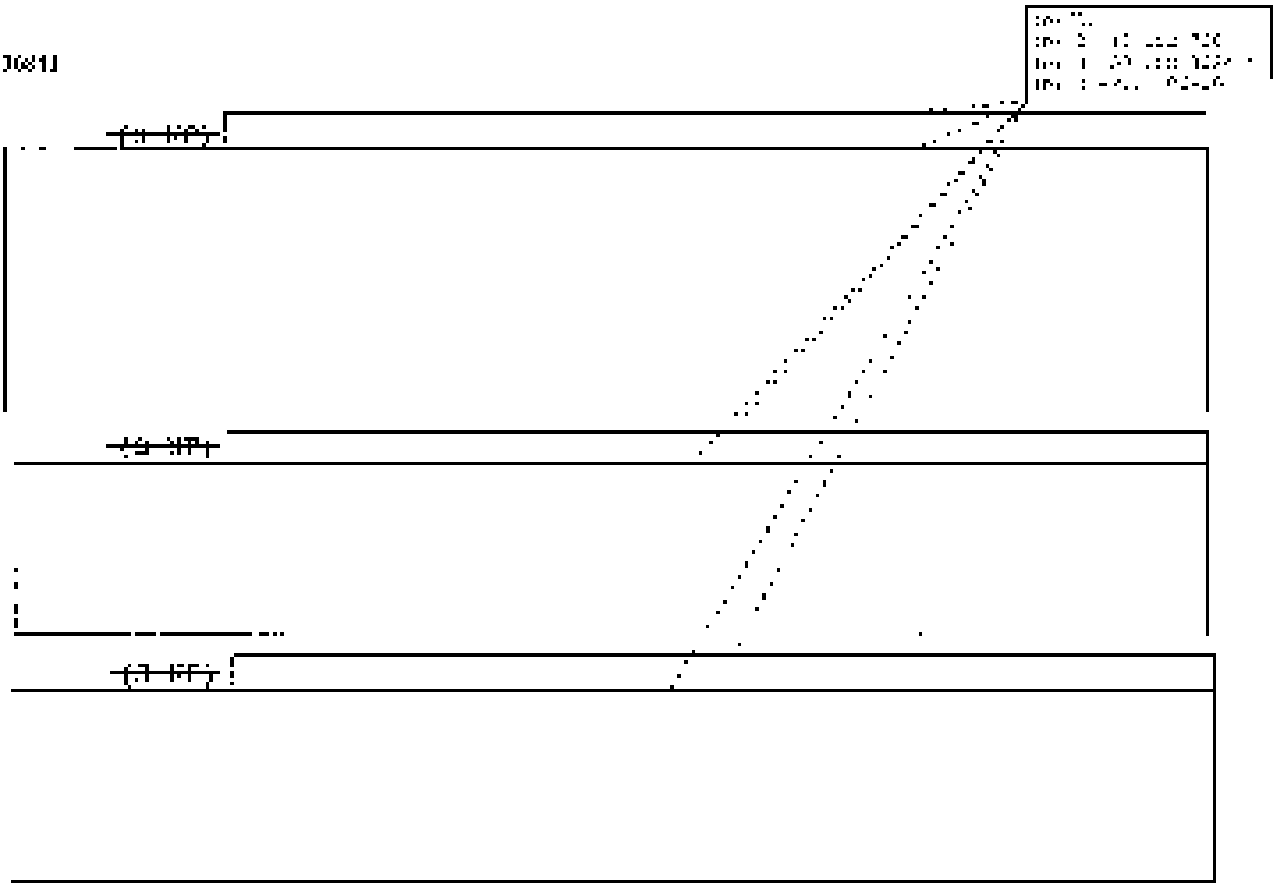
[redacted] unique collection from COMO conventional sites, [redacted] US resources; use of US [redacted] where the US has none; [redacted] the cryptanalytic and interoperability of US & UK SIGINT systems; a strong analytic workforce, with a capability for independent interpretation of events; an especially competent cryptanalytic workforce; savings in US resources by analytic division of efforts; the pooling of resources on key technical projects [redacted] and, perhaps most significant, a record of supporting the US as an ally in confronting world problems.

(S-CCO) Despite these outstanding areas of success, there [redacted]

[redacted]

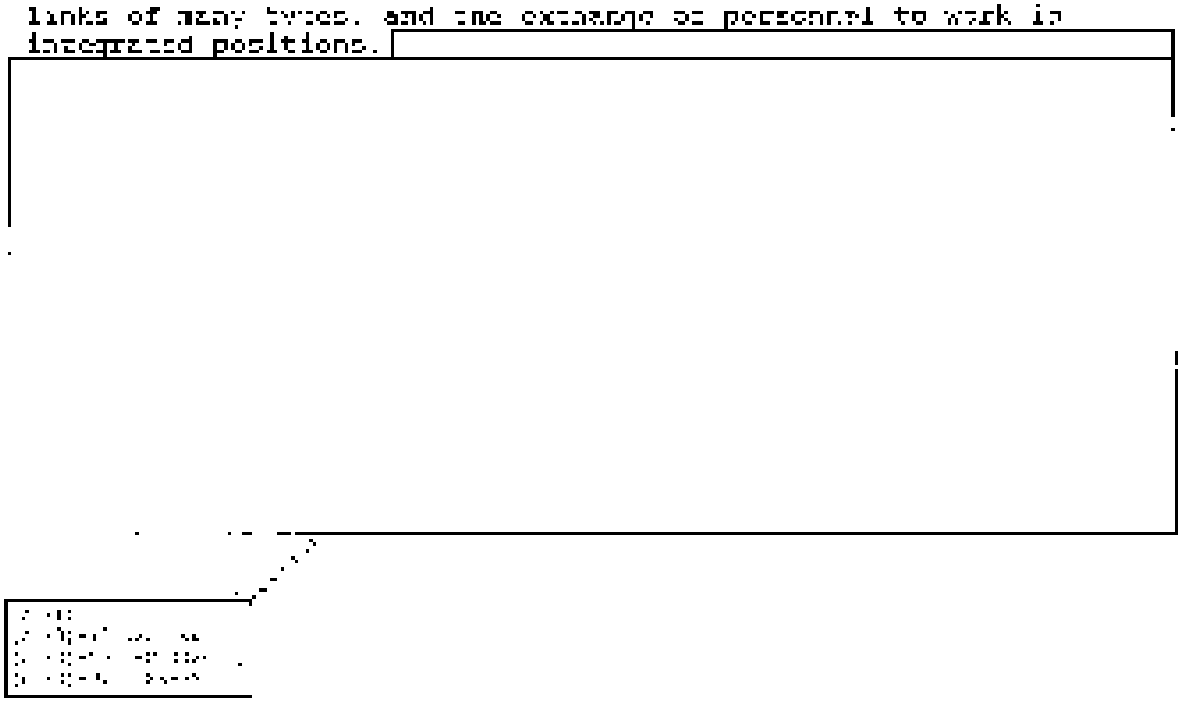
Doc ID: 6618841



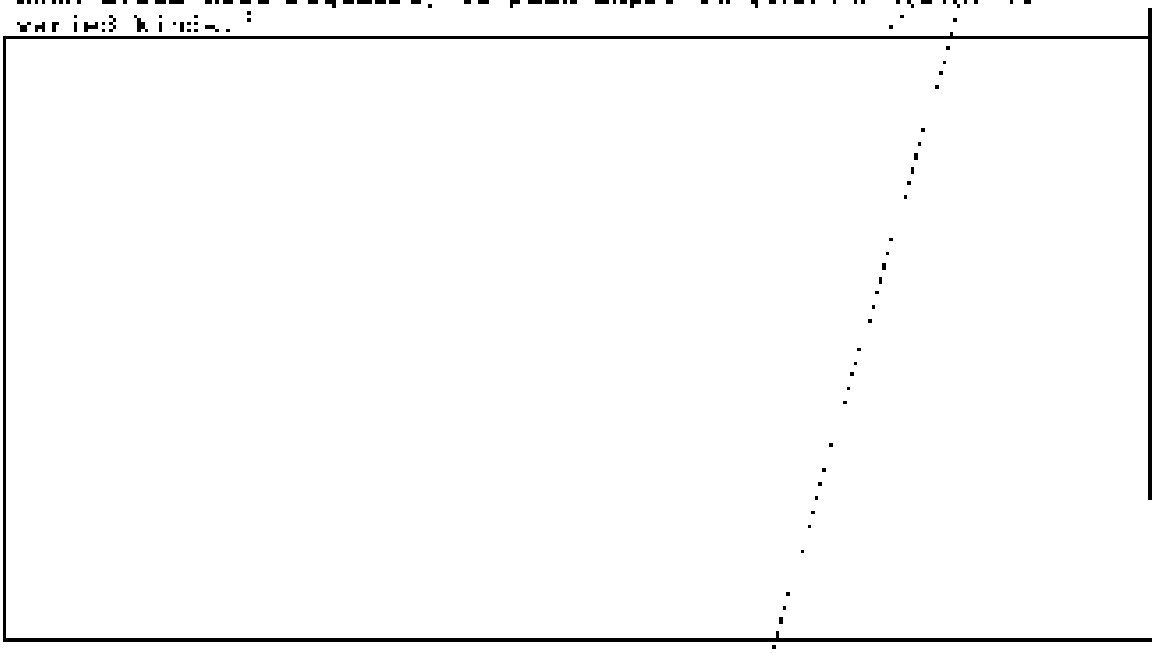


INTERFACES

(C NF) FSA and CCHQ interface in a number of ways, to include connection of joint processing systems, communications links of many types, and the exchange of personnel to work in integrated positions.



(U//FOUO) Communications between NSA and GCHQ run smoothly; both sides meet regularly to plan improved communications of various kinds.



(U//FOUO) Aside from the reciprocal liaison effort, NSA and GCHQ exchange large number of integrees [redacted] NSA/CSS personnel at GCHQ; some [redacted] GCHQ integrees at NSA[redacted]. Most integrees work hard at technical skills and contribute greatly to a mutual interchange of ideals and techniques that benefit both sides greatly. There as in recent years, some operational and staff elements in GCHQ have begun to use integrees as their representatives, and some integrees have assumed liaison-like functions. Making matters worse has been a recent trend to send integrees to function as special assistants, sometimes in eight-to-one components working sensitive missions. While they are no doubt of great help to NSA managers, they also serve as lobbyists for GCHQ seniors in getting matters [redacted]. Recently GCHQ/SIS lobbied hard to place an integree in the W/SA position. It rightly rejected this as it would give GCHQ insight into certain sensitive operations we do not share. In another instance a strategically placed GCHQ integree drafted an NSA that committed [redacted] assistance from NSA to GCHQ -- without addressing the correctness of this arrangement, the propriety of this situation is disturbing.

(U//FOUO) Whether cross links or exchange of integrees, the most of interacting with GCHQ evolves around a myriad of decisions at various levels within NSA. Do we need to have an overall policy to ensure that these agreements are consistent with our plans for the future? For instance, should we determine a modus vivendi for exchange of integrees? Should the type of work be limited by charter? Should there be a common NSA position on the number and kind of electronic interfaces between NSA and GCHQ? Should the number be driven by NSA design or by GCHQ needs?

Declassified

SECRET//COMINT//NOFORN

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

USSID FA6001

(U) SECOND PARTY SIGINT RELATIONSHIPS

ISSUE DATE: 22 August 2012

REVISED DATE:

(U) OFFICE OF PRIMARY CONCERN

(U) National Security Agency/Central Security Service (NSA/CSS)
Foreign Affairs Directorate

(U) LETTER OF PROMULGATION, ADMINISTRATION, AND AUTHORIZATION

(U) Topic of Promulgation	(U//FOUO) USSID FA6001 provides policy and guidance to elements of the United States SIGINT System (USSS) concerning relationships with Second Party SIGINT organizations. While USSID FA6001, "Third Party SIGINT Relationships," dated 31 October 2007 (as of 29 September 2009) provides policy and guidance concerning Foreign Partner relationships, NSA/CSS maintains a close relationship with its SIGINT organizations in Australia, the United Kingdom, Canada and New Zealand by virtue of the British-U.S. Communications Intelligence Agreement (UKUSA), dated 5 March 1946.
(U) USSID Edition	(U) This USSID supersedes USSID FA6001, dated 22 March 1995, which must now be

SECRET//COMINT//NOFORN

destroyed.

(U) Legal Protection of Sensitive Information

(U//~~FOUO~~) This USSID contains sensitive information that is legally protected from release to any member of the general public and is to be used only for official purposes within the NSA/CSS.

(U) Handling of USSID

(U) Users are initially advised of all classification and handling restrictions (see NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Manual," dated 23 November 2004, revised 8 January 2007) when:

- (U) storing hard or soft copies of this USSID; or
- (U) hyperlinking to this USSID.

(U) Users are responsible for the update and management of this USSID when it is stored locally.

(U) Location of Official USSID

(U//~~FOUO~~) The Chief, SIGINT Policy will maintain and update the current official USSID on NSANet (type "go ussid"). Selected USSIDs are also available on an access-controlled INTELINK Web page. Requests for access to the INTELINK USSID Page are granted based on need-to-know. Go to the following INTELINK site: http://sigint.ssg.ic.gov/policy/ussids.cfm

(U) Access by Contractors and Consultants

(U) For NSA/CSS elements to include the SIGINT Extended Enterprise:

(U//~~FOUO~~) USSS contractors or consultants assigned to NSA/CSS Headquarters or to other elements of the SIGINT extended enterprise are pre-authorized for access to a USSID on NSANet or INTELINK (or its Portal-only Internet-based extranet). However, for those sensitive USSIDs for which access is password-controlled, all users, to include contractors, must undergo additional security and mission vetting.

(U) Outside NSA/CSS elements:

(U//~~FOUO~~) Non-USSS contractors or consultants working at sites not facilities are pre-authorized for soft-copy access to USSIDs on NSANet or INTELINK (or its Portal-only Internet-based extranet). However, for those sensitive USSIDs for which access is password-controlled, all users, to include contractors, must undergo additional security and mission vetting.

Where only connectivity is established, any hard-copy provision of USSIDs must be authorized by the Chief, SIGINT Policy (NSA/CSS Secure Telephone System (NSTS): 968-8163, Secure Terminal Equipment (STE): (443) 479-1489, Unclassified

Switched Network (DSN): 689-5467).

(C) Access by Third Party Partners

(U) To request a shareable version:

- (U) Refer to USSID SP0009, Annex B, and
- (U) Contact the appropriate Country Desk Officer in the DoD Branch of the NSA/CSS Foreign Affairs Directorate (FAD).

(U) Executive Agent: (C) The executive agent for this USSID is:

/S//
TERESA H. SHEA
Signals Intelligence Director

(U) TABLE OF CONTENTS

(U) Annexes and Appendices

ANNEX A - (U) SIGINT LIAISON WITH AUSTRALIA, CANADA, NEW ZEALAND, AND THE UNITED KINGDOM

ANNEX B - (C) RELEASE OF U.S. SIGINT INFORMATION TO SECOND PARTY PARTNERS

SECTION 1 - (C) POLICY

(U) Policy

1.1. (U//~~FOUO~~) The SIGINT Director is determined to continue foreign partner cooperation in mutually beneficial relationships, in accordance with U.S. laws and policy, including Director of National Intelligence (DNI) and Secretary of Defense (SECDEF) guidance. The Office of the Director of National Intelligence (ODNI) establishes policy governing procedures for the overall conduct of all SIGINT [redacted] with foreign governments in accordance with DCID 6/5, "Conduct of SIGINT Liaison with Foreign Governments and the Release of U.S. SIGINT to Foreign Governments."

1.2. (U//~~FOUO~~) SIGINT relationships with foreign nations, to include those involving information partners Australia, Britain, Canada, and New Zealand, have historically provided, and must continue to provide, a clear benefit to the United States and as specified in DCID 6/6, "Security Controls on the Dissemination of Intelligence Information," dated 11 July 2001, promote the interests of the United States, be consistent with U.S. law, and take account of potential risks to U.S. foreign policy or national defense. U.S. SIGINT [redacted] cooperation, or collaboration shaped with foreign partners must also enhance U.S. national interests through contributions by the SIGINT partner, support U.S. strategy when SIGINT is to be shared, and contribute to U.S. defense and intelligence goals.

(U) Executive Agent

1.3. (U//~~FOUO~~) The National Security Agency/Chief, Central Security Service (NSA/CHCSS) executes ODNI policy guidance in the conduct of SIGINT arrangements with Australia, Canada, New Zealand, and the United Kingdom (UK) (hereinafter referred to as Second Parties). The Second Party SIGINT organizations are the Defence Signals Directorate (DSD) for Australia, the Communications Security Establishment Canada (CSEC) for Canada, the Government Communications Security Bureau (GCSB) for New Zealand, and the Government Communications Headquarters (GCHQ) for the UK.

SECTION 2 - (U) RESPONSIBILITIES

~~SECRET//SI//REL TO USA, FVEY~~

(U) DIRNSA/CHCSS

2.1. (U//~~FOUO~~) DIRNSA/CHCSS, with the approval of the ODNI, accredits a Special United States Liaison Officer (SUSLO) for each Second Party SIGINT organization. Each SUSLO is responsible for SIGINT liaison and exchange with the appropriate accredited Second Party SIGINT organization. The SUSLO represents the ODNI and DIRNSA/CHCSS in all SIGINT relationships with the Second Party, and must do so in accordance with National Intelligence Board (NIB) policy guidance.

2.2. (U//~~FOUO~~) The SUSLO facilitates the exchange of information to ensure that SIGINT mission needs and SIGINT information requirements of the appropriate Second Party SIGINT organization are met. The SUSLO also advises in many SIGINT matters and sets the type of collaboration between NSA elements and their Second Party counterparts.

(U) NSA/CSS Organizations

2.3. (U//~~FOUO~~) The NSA/CSS Associate Directorate for Policy and Records (DC) is responsible for the staff administration of the policies and procedures established in this USSID.

2.4. (U//~~FOUO~~) NSA/CSS Mission Delegation Authorities (MDAs) provide Mission Authorities (MAs) and supporting Mission Management Officials (MMOs) overseeing the release of SIGINT materials.

SECTION 3 – (U) GENERAL

(U) U.S. – Second Party Collaboration

3.1. (U//~~FOUO~~) U.S.-Second Party collaboration includes [redacted] planning for emergencies, wartime operations, and combined exercises and training and encompasses SIGINT operations conducted by DIRNSA/CHCSS and the Second Party involved.

3.2. (U//~~FOUO~~) SIGINT functions, organizations, and technology of each of the Second Parties, using Dispatch Logic, vary greatly and dictate specific procedures.

(U) Access to U.S. SIGINT

3.3. (U//~~FOUO~~) To access U.S. SIGINT information, Second Party personnel must meet and comply with all U.S. legal, security, oversight, and training guidelines. Access by a Second Party personnel to U.S. SIGINT Program materials or U.S. SIGINT information is permitted only when the following criteria are met: Communications Intelligence (COMINT) exclusive and subsidiary access authorization have been validated using liaison channels, and the request for access has been approved by the individual's parent organization. NSA/CSS is the final approving authority for Second Party access in accordance with Signals Intelligence Directive (SID) Management Directive (SMD) 421, "Access to Data or Non-U.S. Party Personnel Engaged in SIGINT Production," dated

Doc ID: 6606713

[redacted]

1 August 2006.

SECTION 4 - (U) TECHNICAL EXCHANGE AND VISITS

(U) Technical SIGINT Material Exchange

4.1. (U//FOUO) Technical SIGINT (SIGINT) is exchanged between U.S. and Second Party parties on U.S. visits in accordance with the provisions of USSID CR1400, "Technical Electronic Intelligence (ELINT) Signals Analysis, and Data Forwarding Procedures," dated 25 April 2001, and the forwarding instructions of the most respective year's USSID.

4.2. (U//FOUO) [redacted]

(U) Visits and Engagements

4.3. (U//FOUO) Proliferation and availability of secure communications technology provides numerous opportunities to acquire and exchange information that were previously unavailable. While such visits and engagements in support of USSS programs will be encouraged and supported, requests to convey and exchange information will be necessarily approved based on the following criteria:

a. (U//FOUO) The visit fulfills a requirement that cannot be satisfied through other established liaison channels.

b. (U//FOUO) The visit of the visiting party will contribute to the stated purpose of the visit and be accommodated by the host facility.

c. (U//FOUO) The cost of the visit is reasonable in the long run.

d. (U//FOUO) The visit is mutually beneficial.

4.4. (U//FOUO) Visits between USSS elements (including temporary and Second Party liaison personnel assigned to the parties' locations) will be established below. The Chairman of the Board AND the representative to be visited (depending on which procedure is to be followed):

4.5. (U) Second Party personnel visiting U.S. SIGINT organizations:

a. (U//FOUO) The visitor must propose the visit through the national SIGINT authority (CSEC, DSD, GCSB).

b. (U//FOUO) The national SIGINT authority will forward the visit request to [redacted]

EXCEPTION 1: (U//[redacted]) For cleared U.S. personnel locally (for example, SUSLO Ottawa) proposing TDY travel to U.S. SIGINT facilities in Europe, SUSLOO and SUSLOW respectively handle proposed Australian and New Zealand personnel visits to U.S. SIGINT facilities in the Pacific).

EXCEPTION 2: (U//[redacted]) For visits to the Cryptologic Centre – Exceptional SIGINT authority will forward the visit proposal and clearance verification to [redacted]

U.S. CRYPTOLOGIC personnel visiting Second Party facilities:

- (U) Visits to Second Party facilities within Second Party national borders:
  - (U) Point of contact should forward visit proposal and clearance verification message to:
    - (U//[redacted]) Special United States Liaison Officer, London (SUSLOL) and SUSLOL, Cheltenham (SUSLOL CHELT) for visits to the UK;
    - (U//[redacted]) Special United States Liaison Officer, Ottawa (SUSLOO) for visits to Canada;
    - (U//[redacted]) Special United States Liaison Officer, Canberra (SUSLOC) for visits to Australia; and
    - (U//[redacted]) Special United States Liaison Officer, Wellington (SUSLOW) for visits to New Zealand.
  - (U//[redacted]) Should be included on distribution for all such visit proposals, but is no longer required to show concurrence on each visit request.
  - (U//[redacted]) The agency/organization (Program Management Office) that is the host for all such visit proposals.
  - (U//[redacted]) [redacted]
  - (U//[redacted]) The SUSLO will coordinate with Second Party Partners for these visits.
- (U//[redacted]) Visits to Second Party facilities based outside the Second Party national borders:

- (U//FOUO) The visitor should contact the appropriate Second Party country CSCO or DP for guidance early in the visit arrangement process.

4.7 (U//~~FOUO~~) U.S. service cryptologic personnel visiting in-theater Second Party SIGINT facilities:

[redacted]

- (U//~~FOUO~~) [redacted] as appropriate their NCA concur/approve visits including policy issues.

4.8. (U//~~FOUO~~) Other U.S. government personnel visiting Second Party SIGINT facilities:

a. (U//~~FOUO~~) Visits to Second Party SIGINT organizations:

- (U//~~FOUO~~) The visitor must prepare the visit and forward the clearance to DP, who will coordinate with [redacted] and forward the approval to the proper SSO/CSO.

EXCEPTION (U//~~FOUO~~) In-theater visits should be processed locally. For example, United States European Command (USEUCOM) visits to U.K. SIGINT facilities will be proposed directly to SUSLOC, United States Pacific Command (USPACOM) visits to Australia or New Zealand SIGINT facilities should be processed directly to SUSLOC and SUSLOW respectively.

- (U//~~FOUO~~) All visit proposals must be formally approved by the Second Party partner, the forwarding of a clearance does not constitute visit approval. DP or SUSLO will notify visitors of approval when received from the Second Party.

b. (U//~~FOUO~~) Visits to Second Party government facilities/activities that are not intelligence collection related:

- (U//~~FOUO~~) If the visit is to a military facility, visitor should forward a visit proposal and clearance certification message directly to the Staff Security Officer (SSO) of the Second Party military component as follows:

[redacted]

  - (U//~~FOUO~~) For visits to UK military facilities, send a message to Dutch [redacted]
  - (U//~~FOUO~~) For visits to Canadian military facilities, send a message to

- ~~(U//FOUO)~~ For visits to Australian military facilities, send a message to
- ~~(U//FOUO)~~ For visits to New Zealand military facilities, send a message

- ~~(U//FOUO)~~ If the visit is to a military facility, the visitor and DIB sponsor visit proposal and clearance certification messages as follows:
  - ~~(U//FOUO)~~ For visits to U.K. military facilities, send a message to SUSLO LONDON UK with a multi-addressee copy to NSA C06;
  - ~~(U//FOUO)~~ For visits to Canadian military facilities, send a message to SUSLO OTTAWA;
  - ~~(U//FOUO)~~ For visits to Australian military facilities, send a message to SUSLO CANBERRA;
  - ~~(U//FOUO)~~ For visits to New Zealand military facilities, send a message to SUSLO WELLINGTON.

4(b) ~~(U//FOUO)~~ U.S. contractor visiting Second Party SIGINT entities for SIGINT discussions.

- ~~(U//FOUO)~~ The contractor must have an NSA/CSS sponsor.
  - ~~(U//FOUO)~~ If the contractor is working jointly with a Second Party SIGINT organization and does not have an NSA/CSS sponsor, DIB will CHOP the NSA/CSS sponsorship.
  - ~~(U//FOUO)~~ The NSA/CSS sponsor is responsible for verifying clearances and forwarding the visit proposal and clearance certification message to the appropriate SUSLO(s).
  - ~~(U//FOUO)~~ Include the NSA/CSS Office of Industrial and Acquisition Security (Q13) on distribution for all contractor visit messages.

~~(U//FOUO)~~ Second Party cryptologic personnel and their contractor representatives visiting U.S. contractor facilities for SI level discussions:

~~TOP SECRET//COMINT//NOFORN//20291123~~

h. (U//~~FOUO~~) DP will brief on any conditions required in the event.

i. (U//FOUO) The NSA/CSS Special Security Organization will complete the Clearance Certification Form (Form G2901) and forward it to DP for signature; and

- (U//~~FOUO~~) If NSA/CSS is not accessing the visit via appropriate channels, a Courier must complete form G2901 and forward it to DP for signature.

j. (U//~~FOUO~~) DP will sign the form and forward it to the NSA/CSS Special Access Office (Q23).

(U//~~FOUO~~) Visit Proposal Messages

[redacted] (U//~~FOUO~~) All visit proposal messages must be forwarded and contain the following visitor information:

[redacted]

SECTION 5 - (U) COMBINED PARTIES AND INTEGRATED PERSONNEL ASSIGNMENTS

(U) SIGINT Agreements

5. (U//~~FOUO~~) Agreements between USCSS/CCIS-S and Second Party SIGINT organizations provide for the reciprocal exchange of personnel, operations, and research efforts and integrated personnel assignments at SIGINT locations.

(U) Second Party Integration

6. (U//~~FOUO~~) In accordance with NSA/CSS Policy 1-10, "Second Party Integrees," dated 29 December 2010, the integration of Second Party personnel into USCSS sites will

Declassify On: [redacted]

~~SECRET~~//REL TO USA, FVEY

for support when it is beneficial to the U.S. SIGINT mission. The establishment of these positions must be coordinated with, and approved by DF prior to staffing actions within NSA/CSS.

(U) Security Ramifications

5.2. (~~S//SI~~//REL TO USA, FVEY) Security ramifications of [redacted] necessitate that Second Party integrees: 1) be fully read-on prior to gaining access to NSA/CSS facilities, and 2) sign any applicable agreements in accordance with NSA/CSS Policy 1-13 and SMD-123. Second Party integrees should not be placed in positions where they might influence or represent the U.S. SIGINT decision making process, including both command and policy determinations.

SECTION 6 - (U) SECURITY AND CLASSIFICATION

(U) SIGINT Security Procedures

6.1. (~~S//SI~~//REL TO USA, FVEY) SIGINT security procedures and criteria are mutually agreed to by U.S. and Second Party policy authorities and are contained in USSID SE003.

(U) Classification

6.2. (~~S//SI~~//REL TO USA, FVEY) As of December 1981, the Fort Gordon DENSA/CCSS has a relationship with two of all Second Party countries, in that they exchange liaison officers and conduct liaison concerning SIGINT. It is classified [redacted]

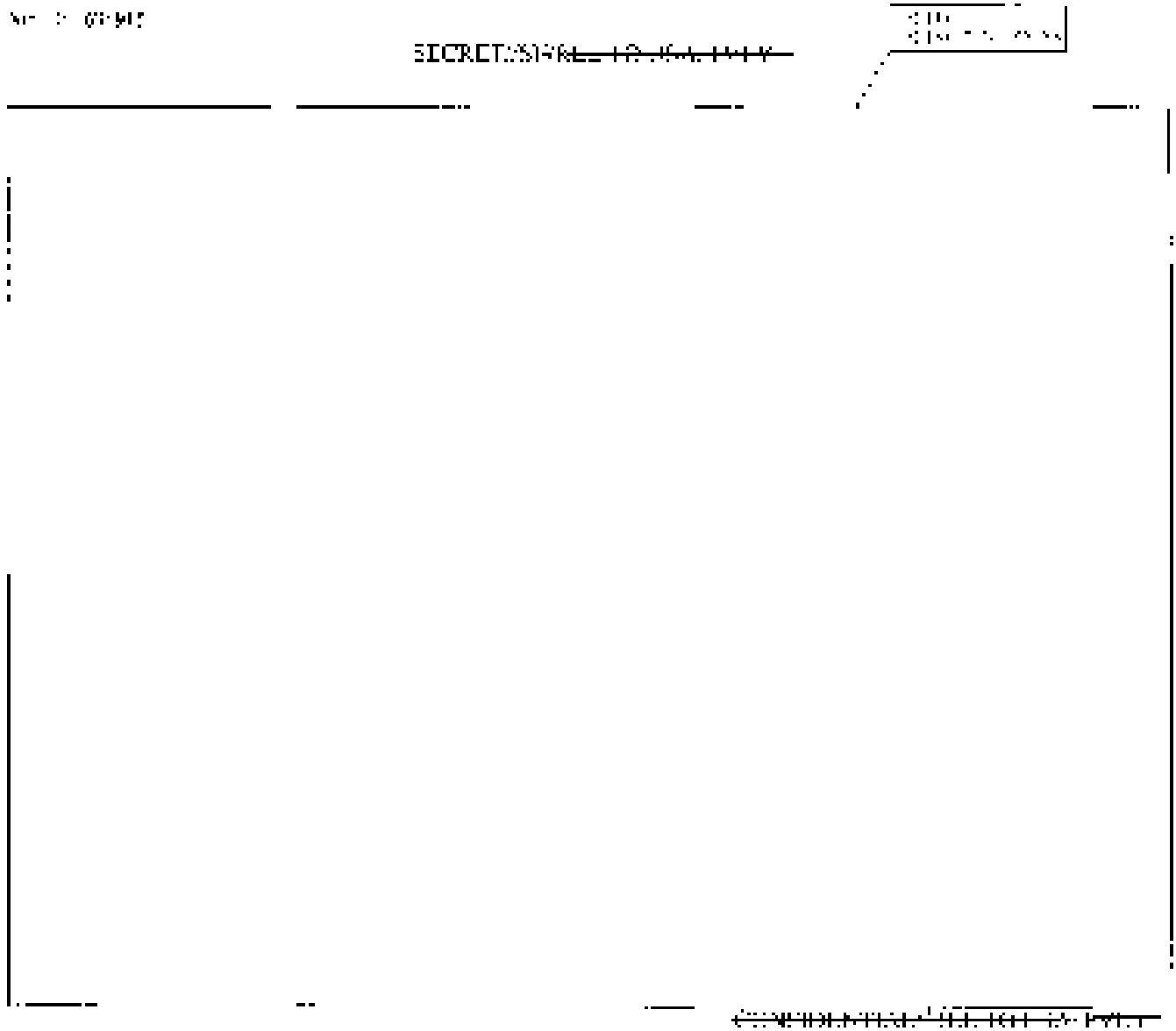
SECTION 7 - (U) SECOND PARTY SIGINT ORGANIZATIONS AND LIAISON OFFICES

(U) Second Party SIGINT Organizations

7.1. (~~S//SI~~//REL TO USA, FVEY) The Second Party locations and liaison offices, and NSA/CSS Liaison offices associated with Second Parties, that appear in NSA/CSS correspondence are:

(~~S//SI~~//REL TO USA, FVEY)

Second Party SIGINT Organizations



USSID FA6001
ANNEX A - (U) SIGINT LIAISON WITH AUSTRALIA, CANADA, NEW ZEALAND, AND THE UNITED KINGDOM

SECTION I - (U) PURPOSE

(U) Purpose 6.1 (U) This Annex delineates procedures and responsibilities for conducting SIGINT

liaison with Second Party collaborating centers.

SECTION 2 - (U) RESPONSIBILITIES

(U) SUSLO

A2.1. (U) The SUSLO, as the senior representative of DIRNSA/CHCSS to the Second Party organization, is responsible for ensuring the continued effectiveness of SIGINT collaboration.

(U) The Associate Director for Policy and Records

A2.2. (U//FOUO) The Associate Director for Policy and Records (ADPR), or [redacted], is responsible for the overall [redacted] foreign relations planning.

(U) Director of Foreign Affairs

A2.3. (U//FOUO) The Director, Foreign Affairs is the principal agent of DIRNSA/CHCSS for supervising the conduct of liaison with foreign partners. Within DF, D41 (SIGINT Operations) is responsible for Second Party SIGINT relations and DP5 is responsible for Second Party cryptologic Assistance relations.

(U) Commanders of the U.S. Service Cryptologic Components (SCCs)

A2.4. (U//FOUO) The commanders of U.S. SCCs, or their respective service representatives, are authorized to conduct liaison with respective Second Party military cryptologic SIGINT units or elements in the area of responsibility (AOR) to exchange technical information, SIGINT operational capabilities, tactics, training, personnel utilization, etc. This includes exchange visits between cryptologic personnel attached to military units and other non-SIGINT organizations.

[redacted]

a. (S//SI//REL) Prior approval for liaison on non-routine SIGINT matters must be coordinated by the SCC through DIRNSA/CHCSS, Respective SCC Headquarters are to [redacted] appropriate SUSLO must be included on all correspondence requesting such approval.

[redacted]

b. (U//FOUO) SCC representatives shall notify, as soon as practicable, any significant [redacted] agreements made, or subjects discussed during such liaison to DIRNSA/CHCSS, the respective SCC Headquarters, D2, and the appropriate SUSLO.

SECTION 3 - (U) PROCEDURES

(U) General

A1. (U//~~FOUO~~) Effective SIGINT liaison between DIRNSA/CHCSS and Second Party Partners requires the use of SUSLOs as the channels to Second Party Partners. Similarly Second Party partner liaison officers must also work with NSA/CSS.

A2. (U//~~FOUO~~) NSA/CSS Headquarters elements use "CIDNSA" (vice NSA) as the "FROM" addressee when corresponding with SUSLOs or Second Party centers.

A3. (U//~~FOUO~~) For all information-related matters (Temporary Duty (TDY), personnel actions, etc.), do not exclude either the Second Party HQ or its liaison office at NSA/CSS as an action or information addressee.

A4. (U//~~FOUO~~) Information Assurance inquiries should be forwarded to the Information Assurance Directorate (IAD) with information copies to DP's SIGINT Operations Group (DP1) and Information Operations Group (DP2). Since this is a UKUSA SIGINT Directive, it is NSA/CSS IAD's recommendation that the information sent to IAD be limited to what has been proposed. IAD documentation should address foreign partner engagement.

(U) Second Party Liaison and Collaboration

A5. (U//~~FOUO~~) The SUSLOs include the SUSLOC (Canberra), the SUSLOG (Gchq) the SUSLOW (Wellington), and the SUSLO (Ottawa). Each SUSLO is to be kept informed of developments that pertain to their country of loc, NSA/CSS and Second Party relationships.

A6. (U//~~FOUO~~) DSD, GCSB, GCSB and GCHQ have established

[redacted]

a. (U//~~FOUO~~) It is necessary to consult Second Party before approaching the SUSLO, advise the SUSLO as soon as possible thereafter. Whenever substantive information is passed orally to a liaison officer, prepare a brief memorandum for the record of the conversation, and forward copies to the SUSLO, DIRNSA/CHCSS, DP, and DP2 or IA, by the most expeditious means.

b. (U//~~FOUO~~) Refer to the appropriate Second Party liaison office all replies to queries or actions from that office, even if the correspondence responds to a communication that has been forwarded from the director or chief of a Second Party HQ. Such correspondence must be coordinated with DP prior to release. For all information copies to the SUSLO, mark it

Doc ID: 6626015

~~TOP SECRET//COMINT//NOFORN~~

USSID FA6001
ANNEX B - (U) RELEASE OF U.S. SIGINT INFORMATION TO SECOND PARTY SIGINT ORGANIZATIONS

SECTION 1 - (U) PURPOSE

(U) Purpose

(U) This Annex sets forth the procedures for releasing U.S. SIGINT information to the Second Party SIGINT organizations.

SECTION 2 - (U) GENERAL

(U) Second Party Collaboration

(S//SI//REL TO USA, FVEY) NSA/CSS and the Second Party Partners collaborate on a wide range of targets. The specific targets and degree of collaboration may change from time to time by mutual agreement and should be documented by a Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) or a Division of Effort (DOE) statement. Copies of all MOU/MOAs must be provided to the NSA/CSS Office of Corporate Policy (DJ), DP and SID SIGINT Policy. If a DOE Statement between NSA/CSS and Second Party elements is used for coverage of a specific target, a copy of this agreement must be provided to DP1.

(U) SIGINT Material

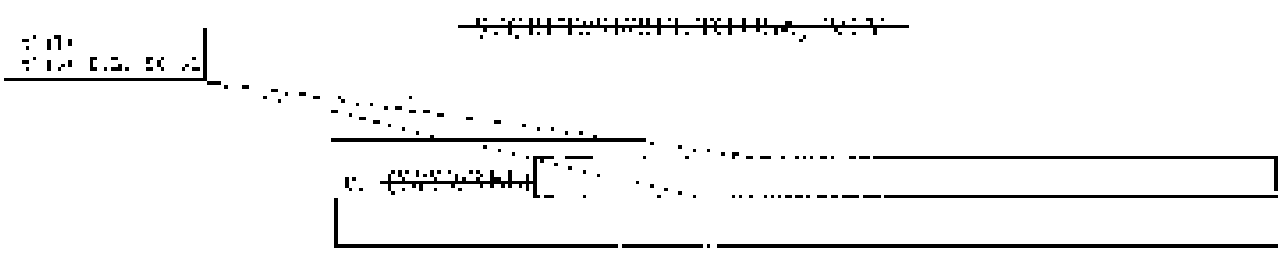
(S//SI//REL) Second Party Partners may release to other authorized recipients SIGINT reports derived from the U.S. effort on mutual targets in accordance with U.S. government policy and guidelines as set forth in USSID 403, as applicable.

(U) Intelligence Information Requirements

(S//SI//REL) Second Party Partners require insight into the U.S. process of inspecting communications related to, and accessing, selected foreign entities, activities, infrastructures, or economic interests. However, no U.S. SIGINT information will be used or disseminated by Second Party Partners in a way that contradicts U.S. government policy and national security goals and objectives or is inconsistent with U.S. law. In addition to established reporting formats set by Second Party Partners to meet customer intelligence requirements, communications may be given to:

a. (S//SI//REL)

b. (S//SI//REL)



SECTION 3 - (U) RESPONSIBILITIES

(U) NSA/CSS Senior Management

D3.1. (U//~~FOUO~~) NSA/CSS Deputy Directors/Associate Directors/Chiefs are responsible for ensuring compliance with established procedures when releasing SIGINT material under the purview to Second Party Partners. They are also responsible for providing any information/permissions requested.

(U) Information Sharing Services

D3.2. (U//~~FOUO~~) NSA/CSS SID Information Sharing Services (S12) maintains records of sanitized reports, including field-produced sanitized reports, that are released to Second Party Partners. Any release that violates established thresholds or guidelines must be coordinated with S12 and DDI. S12 will review SIGINT sanitizations with Second Party Partners that are to involve the release of high-interest or gray-area information.

SECTION 4 - (U) PROCEDURES

(U) Release of SIGINT Material

D4.1. (U//~~FOUO~~) SIGINT material released to the requirements of a Second Party Partner is directly forwarded to the partner location.

D4.2. (U//~~FOUO~~) Release of new categories or types of SIGINT material is to be coordinated with DDI and S12.

D4.3. (U//~~FOUO~~) If U.S. SIGINT material is requested by a particular Second Party Partner, it cannot be released but will be considered upon request by the producer, providing or supporting agency. S12 will review the need and coordinate with DDI.

Proponent Title:
NSA Director | SID | SID Staff | SID Policy | CSSD Index

~~CONFIDENTIAL//COMINT//REL TO USA, FVEY~~

SIGNALS INTELLIGENCE DIRECTORATE

MANAGEMENT DIRECTIVE 427

Issue Date: 01 August 2009
Revised Date: 28 December 2013
Second Rev: 14 September 2015

POC: S02

(U) ACCESS TO CLASSIFIED U.S. INTELLIGENCE INFORMATION FOR SECOND PARTY PERSONNEL

(U) Purpose

(U//~~FOUO~~) This document provides guidance for granting Second Party SIGINT personnel access to Classified U.S. intelligence information in accordance with Department of Defense Directive (DoDD) C-5230.23, "Intelligence Disclosure Policy" (Ref A); Director of Central Intelligence Directive 6/7, "Intelligence Disclosure Policy" (Ref B); [redacted]; and "DoD 5240.1-R, Procedures Governing Intelligence Components that Affect U.S. Persons" (Ref C).

NOTE: (U) Underlined terms are defined under Annex D: Definitions.

(U) Scope

(U) This Signals Intelligence Directorate (SID) Management Directive applies to all U.S. SIGINT personnel at all locations, to include NSA Headquarters (NSAW) and all elements of the United States SIGINT System (USSS).

(U) This guidance supersedes all previously approved SIGINT Directorate guidance and authorizations for Second Party access to classified U.S. intelligence information. Second Party personnel who will be [redacted] and its performance of the SIGINT mission must be re-justified and coordinated for approval by the SIGINT Director or Deputy Director.

Doc ID: 6504610

~~CONFIDENTIAL//REL TO USA, FVEY~~

(U) A new signature for Second Party processing that is not addressed in this Directive must follow the guidelines herein.

/ps/

KEITH B. ALEXANDER
Signals Intelligence Director

DISTRIBUTION:
Signals Intelligence Directorate, A1
SIGINT Enterprise Board, A
Office of General Counsel
Office of Corporate Policy

(U) BACKGROUND

(U) Background

1. (U) NSA/CSS has a tradition of signals intelligence (SIGINT) collaboration with its Second Party SIGINT Partners that has served us well. NSA/CSS and the Intelligence Community (IC) have benefited from this exchange and have bolstered and improved U.S. knowledge base. By upholding our special partnerships without Second Party SIGINT Partners, NSA/CSS must first ensure that activities with our partners comply with all U.S. legal and policy guidelines. This management directive is established to define, document, and implement a framework by which NSA/CSS activities must be in accordance with all legal and policy guidelines.

2. (U) Granting access to Second Party personnel to classified U.S. intelligence information must be done in accordance with procedures established with NSA/CSS in consultation with policies and procedures of the Director of National Intelligence and the Secretary of Defense. In addition, NSA/CSS, first and foremost, has a responsibility to protect intelligence information that contains or may contain equities of other members of the IC. Granting access to appropriately cleared Second Party personnel to unevaluated U.S. SIGINT as well as to intelligence gathered under the authority of other IC agencies, or any intelligence from those agencies, that is fused with SIGINT for analytic purposes (normal alternative access efforts). Often, only the originating agency or element may be aware of the authorities of the intelligence information and that agency's permission must be obtained prior to sharing.

~~CONFIDENTIAL//SI//REL TO USA, FVEY~~

3. (U//~~FOUO~~) The Director of Central Intelligence Directive (DCID) 6/6P, "Conduct of Liaison with Foreign Governments and Release of U.S. SIGINT to Foreign Governments" (Ref D), DIRNSA/CHCSS is designated as the point of contact for the US Government for the conduct of SIGINT arrangements with the Second Parties. DCID 6/6, "Security Controls on the Dissemination of Intelligence Information" (Ref E) specifies that intelligence may be shared with foreigners, including Second Party personnel, when it is determined that the release is in the interests of the United States, is consistent with U.S. law, does not pose unacceptable risk to U.S. foreign policy or national defense, and is limited to a specific purpose and recipient of limited duration. The directive mandates NSA/CSS' responsibility to apply appropriate controls to our relationship to the release of classified intelligence. Foreign partners

(U) Data Categories

4. (U//~~FOUO~~) For the purposes of this policy, data, databases and data sets maintained by NSA/CSS will be categorized as follows:

[redacted]

(U) POLICY

(U) Approval Authorities

5. (U//~~FOUO~~) [redacted]

6. (U//FOUO)

7. (U//FOUO) If a Second Party person is an invitee as defined in USSID 18, Section 10, "Second Party Integrees" (Ref.), then vi. be escorted by the integree's supervisor and the appropriate Foreign Affairs Directorate desk officer at the Directorate

8. (U//FOUO) Second Party personnel access to NSANet non-mainstream data sets or data sets that only contain classified information marked releasable to the parties' citizens (i.e., capable of restricting access only to that data which is marked releasable to that partner, regardless of the originating source of the data), will be granted to Second Party personnel in accordance with Annex A to this policy. Approval authority for Second Party access marked releasable (NOFORN) to the U.S. and SIGINT Director, Deputy Director, Associate Director (ADs), ADDEVs/ADDNMs, DIA DIACDIAP, DDDIA/ADDDIA, and ADD/SSGs; NTOC DDs; and SUSLOs Canberra, London, Ottawa, and Wellington).

9. (U//FOUO)

10. (U//FOUO)

~~CONFIDENTIAL//SI//REL TO USA, FVEY~~

[redacted]

11. (U//~~FOUO~~) The NSA/CSS Director, the NSA/CSS Deputy Director, or authorized Designated Intelligence Disclosure Officers (DIDOs) may authorize release to a Second Party [redacted] specific central intelligence [redacted] marked with "NOFORN," "REL TO," or another control marking such as "ORCON"). The details of this DIDO [redacted] and authorities may be found in DCID 6/7, "Intelligence Disclosure Policy," and the list of designated NSA/CSS DIDOs.

(U) Data Flow

12. (U//~~FOUO~~) Access to data by or release of data to Second Party personnel does not convey authorization or approval for second party [redacted] Further use guidance will accompany each Second Party [redacted]

[redacted]

(U) Termination of Access

15. (U//~~FOUO~~) When a Second Party person changes work assignments or leaves and any access to NSA/CSS maintained data sources or databases granted through an NSA/CSS approval process (such as the SIGINT Digital Gateway (SDG)) should be promptly terminated, in accordance with SID Management Directive 421, "United States SIGINT System Database Access" (Ref TT).

(U) Emergencies

16. (U) For emergency tasking authorization, the NSA Director or Deputy Director and/or the SIGINT Director and Deputy Director are the sole approving authorities. Emergency situations are defined and will be implemented per guidance in USSID 6, Section 10.

(U) ANNEX A
ACCESS TO RELEASABLE DATA

(U) General

A. (U//~~FOUO~~) Second Party personnel, who have integrated into an NSA/CSS established SIGINT production element or assigned to a Second Party SIGINT organization, may be granted access to NSA/CSS maintained SIGINT databases and data sets that contain only content marked as releasable to that Second Party partner and shares the same organizational reporting responsibility as that data which is marked releasable to that partner. All Second Party personnel accessing NSA/CSS maintained databases and data sets must adhere to the same standards as U.S. SIGINT personnel with regard to U.S. intelligence oversight to include U.S. Intelligence Oversight Officers (IOOs), U.S. auditors, and appropriate audit and oversight mechanisms. Reporting produced by Second Party Integrees shall not be released to third parties for which access to NOFORN information is routinely required, without prior approval from all originators of that information.

(U) Access for Personnel in Second Party SIGINT

A.2. (U//~~FOUO~~) Second Party SIGINT accounts requiring access to the Station or collaborative data sets must first be registered in the NSA/CSS Mission Data Station Table (MDST) in accordance with SID Management Directive 422, "NSA/CSS Mission Data Stations" (Ref U), by allowing the SID SIGINT Director

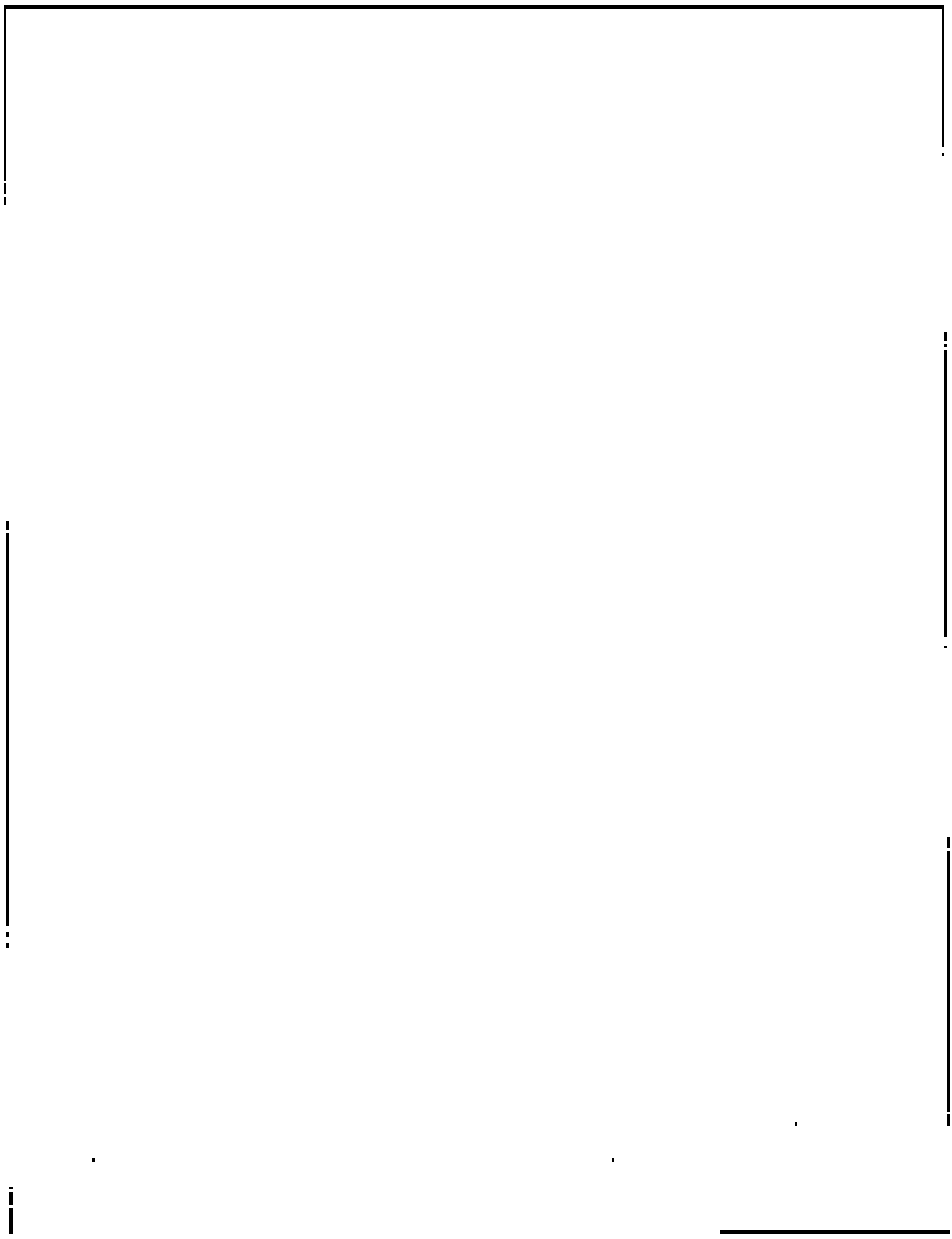
~~CONFIDENTIAL//USA/FVEY~~

Elements	Center (SCC) process [redacted] for Sponsor and Data Waiver approval process. The Second Party mission, the relevant Mission Delegation Group Capability Manager will coordinate on but not approve the registration of the mission and the associated databases.
[redacted]	A.1. (U//~~FOUO~~) Second Party SIGINT elements will work with the appropriate Service/US [redacted] and the appropriate NSA/CSS Foreign Affairs Directorate (FAD) Desk Officer to draft and coordinate the access request for registration in the MCT. The FAD Desk Officer will function as the Sponsor for the SCC process. The Desk Officer will work with SID Oversight and Compliance (O&C) [redacted] to determine the appropriate oversight, training, and auditing requirements for each element and associated database being registered in the MCT. If access is approved, access for individual [redacted] will be granted through the SCC standard procedures.
(U) Access for Second Party Integrees	A.1. (U//~~FOUO~~) Second Party SIGINT personnel integrated into NSA/CSS SIGINT production elements under [redacted] NSA/CSS Policy 1-43, "Second Party Integrees" will be given access to SIGINT through established procedures in SIGINT Management Directive 421. Supervisors of Second Party integrees must maintain a list of any databases or data sets accessed by the integree and will notify the appropriate FAD Desk Officer of any changes during the integree's assignment which would require a change to the Appendix. Approval authority for database access and the "NSA/CSS or IC Requirement" will be the NSA Director, Deputy Director, SIGINT Director or SIGINT Deputy Director.
(U) Termination of Access	A.1. (U//~~FOUO~~) When Second Party personnel no longer work in NSA/CSS facilities, any access to SIGINT databases or data sets will be terminated immediately. The SIGINT production element's NSA/CSS Sponsor or Intelligence Oversight Officer (IOO) is responsible for requesting the database System Administrator to terminate and remove the individual's accounts in the respective mission database with SID Management Directive 421. For Second Party Integrees, the immediate supervisor (U.S. or Second Party) is responsible for the termination of access and will notify the appropriate FAD desk officer and personnel in accordance with SID Management Directive 421.
[redacted]	

(U) ANNEX B

[redacted]

~~CONFIDENTIAL//USA/FVEY~~



(U) ANNEX C
REFERENCES

a. (U//FOUO) Department of Defense Directive (DoDD) C-5230.23, "Intelligence Disclosure Policy"

b. (U//~~FOUO~~) Director of Central Intelligence Directive 6/7, "Intelligence Disclosure Policy"

c. (U//~~FOUO~~) DoDD 5240.01-R, "Procedures of DoD Intelligence Components that Affect U.S. Persons"

d. (U//~~FOUO~~) Director of Central Intelligence Directive (DCID) 5/9, "Conduct of Liaison with Foreign Governments and Release of U.S. SIGINT to Foreign Governments"

e. (U//~~FOUO~~) Director of Central Intelligence Directive (DCID) 6/6, "Security Controls on the Dissemination of Intelligence Information"

(U//~~FOUO~~) NSA/CSS Policy 1-15, "Second Party Integree"

f. (U//~~FOUO~~) NSA/CSS POLICY 1-4, "The NSA/CSS Centrally Controlled Information (CCI) System"

g. (U//~~FOUO~~) SID Management Directive 421, "United States SIGINT System Database Access"

h. (U//~~FOUO~~) SID Management Directive 422, "U.S. SIGINT Mission Delegation"

j. (U//~~FOUO~~) Executive Order (E.O.) 12333, "United States Intelligence Activities"

k. (U//FOUO) [redacted]

l. (U//~~FOUO~~) [redacted] Agreement dated 5 March 1946

(U) ANNEX D
DEFINITIONS

(U) Data Set	D.1. (U) For the purpose of this policy, a large collection of intelligence data that may not be immediately evaluated for foreign intelligence or minimized to protect U.S. identities but is not a finished database supporting the SIGINT Contact Center (SCC) process or a similar process. A data set may also be a data feed such as would be passed for a research/development effort.
(U) Database	D.2. (U//~~FOUO~~) For the purpose of this policy, a structured collection of records or data that is stored in a computer system and organized in a data management system for quick retrieval of those records. A database is typically [redacted] by the SCC process or similar process. [redacted]
(U) Designated Intelligence Disclosure Official (DIDO)	D.3. (U) The Deputy Director and Associate Directors in the Intelligence Directorate (or the Senior National Intelligence Officer (SNIO) in writing, and other [redacted] specifically designated subordinates whose names and positions are certified to the Director National Intelligence (DNI) in writing, and other [redacted] specifically designated by the DNI.
(U) Exceptionally Controlled Information (ECI)	D.4. (U) COMINT has control systems/sub-compartments to protect TOP SECRET exceptionally sensitive COMINT sources, methods and activities.
(U) Evaluated, Minimized Traffic (EMT)	D.5. (U) Traffic that has been minimized for U.S. identities and assessed for foreign intelligence value.

(U) Integree

3.5. (U//FOUO) Electronic Transmission in the Environment of a Second Party Partner. personnel integrated into a designated SIGINT production element (as defined in USSID CR1610) who, when integrated into an NSA/CSS environment, are working jointly under the direction and operational control of the [redacted] to conduct SIGINT activities that support foreign intelligence tasking validated by NSA/CSS in accordance with NSA/CSS authorities, rules, and regulations. Integrees may be civilians or military members. Integrees must be approved in accordance with NSA/CSS Policy 1-16, "Second Party Integrees."

(U) Intelligence

D.7. (U) Includes the following information, whether written or in any other medium, classified pursuant to Executive Order 12958 or any predecessor or successor Executive Order:

a. (U) Foreign intelligence and counterintelligence defined in the National Security Act of 1947 (50 USC 401), as amended and Executive Order 12333.

b. (U//FOUO) Information pertaining to U.S. foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodologies used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from U.S. foreign intelligence collection efforts; and

(U) Information received from foreign governments, foreign organizations, or foreign persons or their agents and that is classified or is determined pursuant to

(U) Intelligence Community (IC)

D.8. (U) The Intelligence Community comprises:

- Central Intelligence Agency (CIA)
- National Security Agency (NSA)
- Defense Intelligence Agency (DIA)
- Bureau of Intelligence and Research (within the Department of State)
- National Geospatial-Intelligence Agency (NGA)
- National Reconnaissance Office (NRO)
- Intelligence and Counterintelligence elements of the Army, Navy, Air Force, Marine Corps, and Coast Guard
- Staff elements of the Director of National Intelligence (DNI), and
- Intelligence elements of the

- Drug Enforcement Administration,
- Federal Bureau of Investigation (FBI),
- Department of Justice,
- Department of the Treasury,
- Department of Homeland Security, and
- Department of Energy.

(U) SIGINT Content

(U) The actual information (e.g., words, data, or video) of a communication between one or more individuals, systems, or devices.

(U) SIGINT Metadata

(U) Data [redacted] that is associated with, but separate from, the content, and includes any data used by a network service, or application to facilitate routing, or handling of a communication or to provide content of the intended format. Metadata includes, but is not limited to, the routing, switching, or processing of signaling information and data in support of various network management activities (e.g. billing, authentication, or tracking of communications).

(U) Mission Correlation Table (MCT)

(U) [redacted]

(U) Product

(U) The [redacted] foreign intelligence product derived from SIGINT processes that is made available or available upon request to authorized recipients in response to stated or implied Intelligence Needs. SIGINT Products reporting standards are governed by United States Signals Intelligence Directives (USSIDs) and other SIGINT policy.

(U) Raw SIGINT Data

(U) [redacted] Raw SIGINT data is any SIGINT data acquired either as a result of search and development or targeted collection operations against a particular foreign intelligence target before the information has been processed into an intelligible report for dissemination and NSA/CSS reporting purposes. It includes, but is not limited to, recordings of unprocessed

[redacted]

(U) Second Party

(U) Second Party SIGINT Partners

(U) Second Party SIGINT Personnel

(U) SIGINT Production Element

~~(S//REL TO USA, FVEY)~~ Any of the four countries with which the U.S. Government maintains close, collective SIGINT and Information Assurance (IA) relationships: Australia, Canada, New Zealand, and the United Kingdom (UK). These strategic alliances among historically like-minded countries from the strong cryptologic partnerships that developed during World War II and were later formalized in the UKUSA Agreement (Ref D), dated 5 March 1946.

~~(S//REL TO USA, FVEY)~~ The following SIGINT organizations are collaborating partners authorized to conduct joint SIGINT operations with the National SIGINT Organizations. These organizations are:

a. (U) UK - Government Communications Headquarters (GCHQ)

b. (U) Canada - Communications Security Establishment Canada (CSEC)

c. (U) Australia - Defence Signals Directorate (DSD)

d. (U) New Zealand - Government Communications Security Bureau (GCSB)

~~(S//REL TO USA, FVEY)~~ Military members of Second Party personnel [illegible] working under the SIGINT Authorities of the respective Second Party Partner organization. This includes Second Party civilian, military, and contractor personnel.

~~(S//REL TO USA, FVEY)~~ Any [illegible] element (organization, entity) that executes at least one of the SIGINT processing functions (collection, processing, analysis, reporting, and dissemination) performed by National Cryptologic SIGINT Systems (NCSS) and/or Foreign SIGINT production systems. Collectors, cryptanalysts, intelligence analysts, linguists, reporters, SIGINT development analysts, research personnel, staff, support elements, and managers necessary for the conduct of an assigned SIGINT mission.

(U) Stakeholder	D.16. (U) Stakeholders in the access of data Not Releasable by a Second Party person would be any office with an equity in the information. This list might include: • SI Customer Relations • SI Analysis and Production • SI Data Acquisition, • SSG SIGINT Development, • Associate Deputy Directorates for Counter Terrorism (ADD/CT) and Technical SIGINT and Electronic Warfare (ADD/TSE), • National Cyber Operations Center (NCOC), • NSA/CSS Commercial Solutions Center (NCSC), • Research Directorate (R4), • Associate Directorate for Education and Training (ADET), • Associate Directorate for Security and Counterintelligence (ADS&CI), and • National Cryptologic Representatives or Senior Liaison Officers, as appropriate
(U) United States SIGINT System (USSS)	D.17. (U) The United States SIGINT System (USSS) is the SIGINT portion of the United States Cryptologic System (USCS) and refers to the U.S. Government SIGINT activities worldwide under the direction of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS). The USSS is composed of the NSA/CSS SIGINT Organization, the SIGINT elements of military intelligence, [redacted], and [redacted] authorized to perform SIGINT activities under the direction and authority of the DIRNSA/CHCSS.

The Guardian

This article is more than **5 years old**

XKeyscore: NSA tool collects 'nearly everything a user does on the internet'

● XKeyscore gives 'widest-reaching' collection of online data ● NSA analysts require no prior authorization for searches ● Sweeps up emails, social media activity and browsing history ● NSA's XKeyscore program – read one of the presentations

Glenn Greenwald

Wed 31 Jul 2013 08.56 EDT

A top secret National Security Agency program allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals, according to documents provided by whistleblower Edward Snowden.

The NSA boasts in training materials that the program, called XKeyscore, is its "widest-reaching" system for developing intelligence from the internet.

The latest revelations will add to the intense public and congressional debate around the extent of NSA surveillance programs. They come as senior intelligence officials testify to the Senate judiciary committee on Wednesday, releasing classified documents in response to the Guardian's earlier stories on bulk collection of phone records and Fisa surveillance court oversight.

The files shed light on one of Snowden's most controversial statements, made in his first video interview published by the Guardian on June 10.

"I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email".

US officials vehemently denied this specific claim. Mike Rogers, the Republican chairman of the House intelligence committee, said of Snowden's assertion: "He's lying. It's impossible for him to do what he was saying he could do."

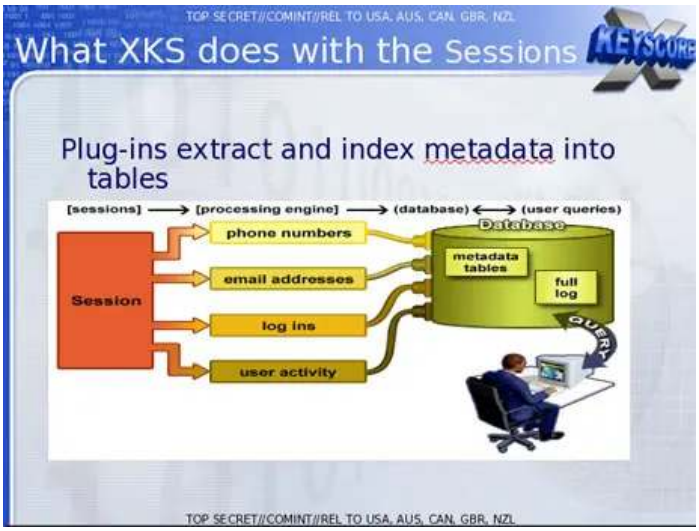
But training materials for XKeyscore detail how analysts can use it and other systems to mine enormous agency databases by filling in a simple on-screen form giving only a broad justification for the search. The request is not reviewed by a court or any NSA personnel before it is processed.

XKeyscore, the documents boast, is the NSA's "widest reaching" system developing intelligence from computer networks – what the agency calls Digital Network Intelligence (DNI). One presentation claims the program covers "nearly everything a typical user does on the internet", including the content of emails, websites visited and searches, as well as their metadata.

Analysts can also use XKeyscore and other NSA systems to obtain ongoing "real-time" interception of an individual's internet activity.

Under US law, the NSA is required to obtain an individualized Fisa warrant only if the target of their surveillance is a 'US person', though no such warrant is required for intercepting the communications of Americans with foreign targets. But XKeyscore provides the technological capability, if not the legal authority, to target even US persons for extensive electronic surveillance without a warrant provided that some identifying information, such as their email or IP address, is known to the analyst.

One training slide illustrates the digital activity constantly being collected by XKeyscore and the analyst's ability to query the databases at any time.



KS1 Photograph: Guardian

The purpose of XKeyscore is to allow analysts to search the metadata as well as the content of emails and other internet activity, such as browser history, even when there is no known email account (a "selector" in NSA parlance) associated with the individual being targeted.

Analysts can also search by name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used.

One document notes that this is because "strong selection [search by email address] itself gives us only a very limited capability" because "a large amount of time spent on the web is performing actions that are anonymous."

The NSA documents assert that by 2008, 300 terrorists had been captured using intelligence from XKeyscore.

Analysts are warned that searching the full database for content will yield too many results to sift through. Instead they are advised to use the metadata also stored in the databases to narrow down what to review.

A slide entitled "plug-ins" in a December 2012 document describes the various fields of information that can be searched. It includes "every email address seen in a session by both username and domain", "every phone number seen in a session (eg address book entries or signature block)" and user activity - "the webmail and chat activity to include username, buddylist, machine specific cookies etc".

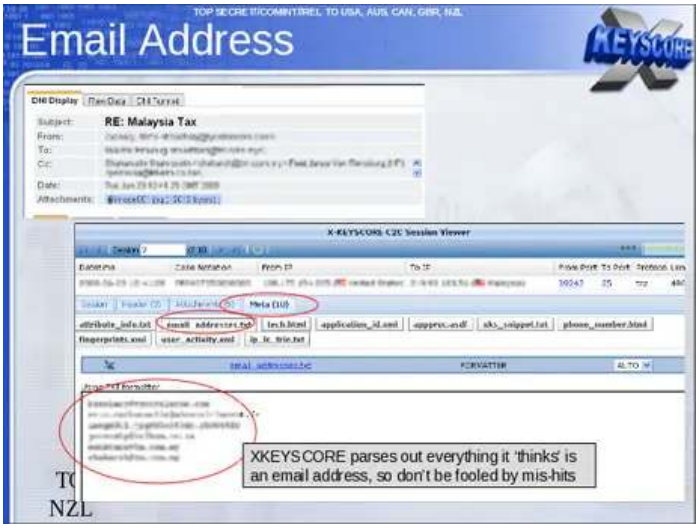
Email monitoring

In a second Guardian interview in June, Snowden elaborated on his statement about being able to read any individual's email if he had their email address. He said the claim was based in part on the email search capabilities of XKeyscore, which Snowden says he was authorized to use while working as a Booz Allen contractor for the NSA.

One top-secret document describes how the program "searches within bodies of emails, webpages and documents", including the "To, From, CC, BCC lines" and the 'Contact Us' pages on websites".

To search for emails, an analyst using XKS enters the individual's email address into a simple online search form, along with the "justification" for the search and the time period for which the emails are sought.

KS2 Photograph: Guardian

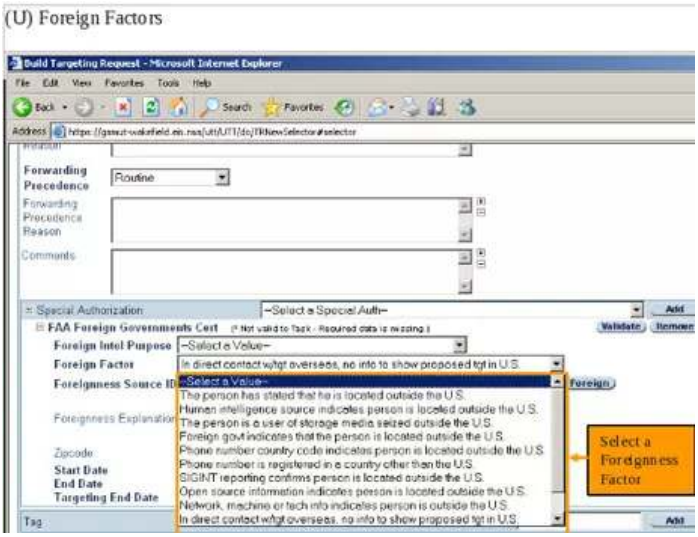


KS3edit2 Photograph: Guardian

The analyst then selects which of those returned emails they want to read by opening them in NSA reading software.

The system is similar to the way in which NSA analysts generally can intercept the communications of anyone they select, including, as one NSA document put it, "communications that transit the United States and communications that terminate in the United States".

One document, a top secret 2010 guide describing the training received by NSA analysts for general surveillance under the Fisa Amendments Act of 2008, explains that analysts can begin surveillance on anyone by clicking a few simple pull-down menus designed to provide both legal and targeting justifications. Once options on the pull-down menus are selected, their target is marked for electronic surveillance and the analyst is able to review the content of their communications:

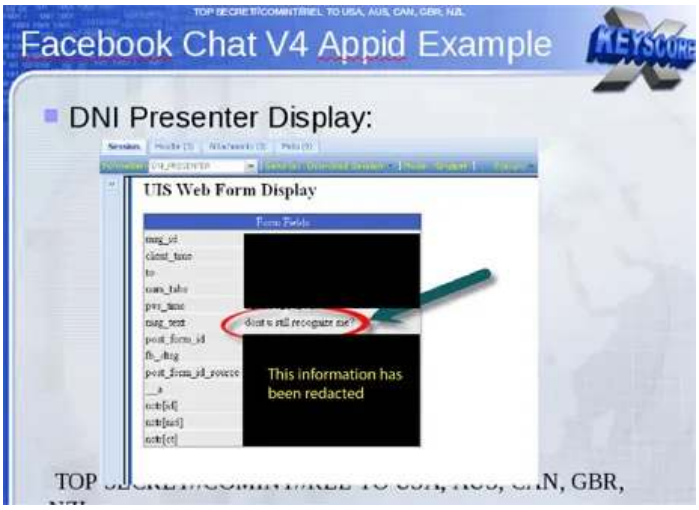


KS4 Photograph: Guardian

Chats, browsing history and other internet activity

Beyond emails, the XKeyscore system allows analysts to monitor a virtually unlimited array of other internet activities, including those within social media.

An NSA tool called DNI Presenter, used to read the content of stored emails, also enables an analyst using XKeyscore to read the content of Facebook chats or private messages.



KS55edit Photograph: Guardian

An analyst can monitor such Facebook chats by entering the Facebook user name and a date range into a simple search screen.

KS6 Photograph: Guardian

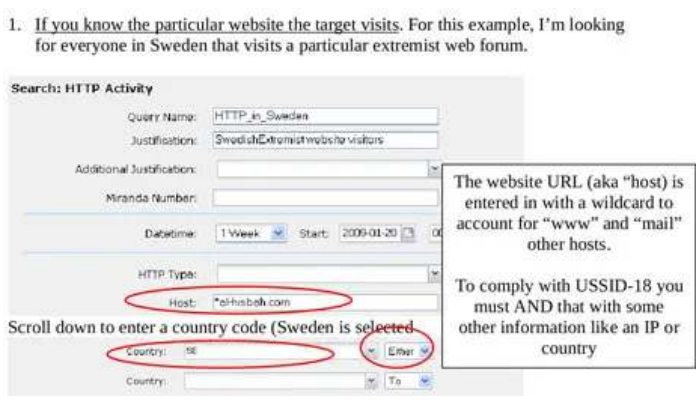
Analysts can search for internet browsing activities using a wide range of information, including search terms entered by the user or the websites viewed.

KS7 Photograph: Guardian

As one slide indicates, the ability to search HTTP activity by keyword permits the analyst access to what the NSA calls "nearly everything a typical user does on the internet".

KS8 Photograph: Guardian

The XKeyscore program also allows an analyst to learn the IP addresses of every person who visits any website the analyst specifies.



KS9 Photograph: Guardian

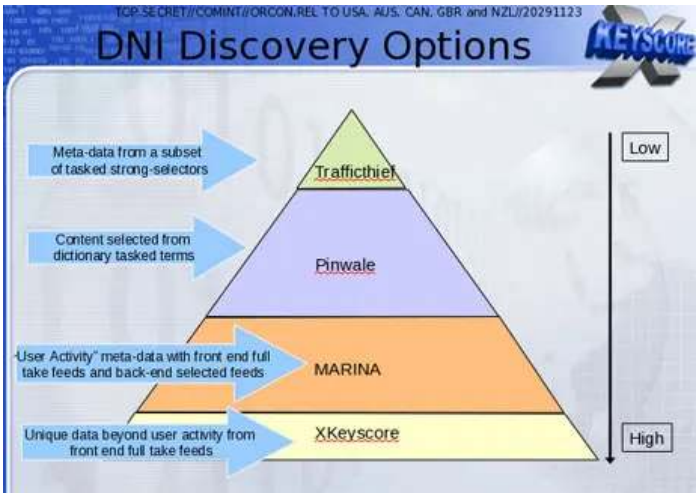
The quantity of communications accessible through programs such as XKeyscore is staggeringly large. One NSA report from 2007 estimated that there were 850bn "call events" collected and stored in the NSA databases, and close to 150bn internet records. Each day, the document says, 1-2bn records were added.

William Binney, a former NSA mathematician, said last year that the agency had "assembled on the order of 20tn transactions about US citizens with other US citizens", an estimate, he said, that "only was involving phone calls and emails". A 2010 Washington Post article reported that "every day, collection systems at the [NSA] intercept and store 1.7bn emails, phone calls and other type of communications."

The XKeyscore system is continuously collecting so much internet data that it can be stored only for short periods of time. Content remains on the system for only three to five days, while metadata is stored for 30 days. One document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours."

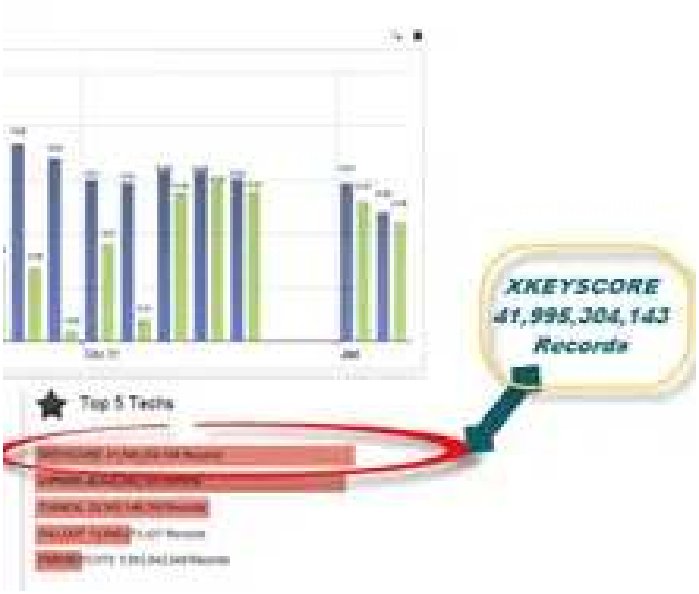
To solve this problem, the NSA has created a multi-tiered system that allows analysts to store "interesting" content in other databases, such as one named Pinwale which can store material for up to five years.

It is the databases of XKeyscore, one document shows, that now contain the greatest amount of communications data collected by the NSA.



KS10 Photograph: Guaridan

In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period.



KS11 Photograph: Guardian

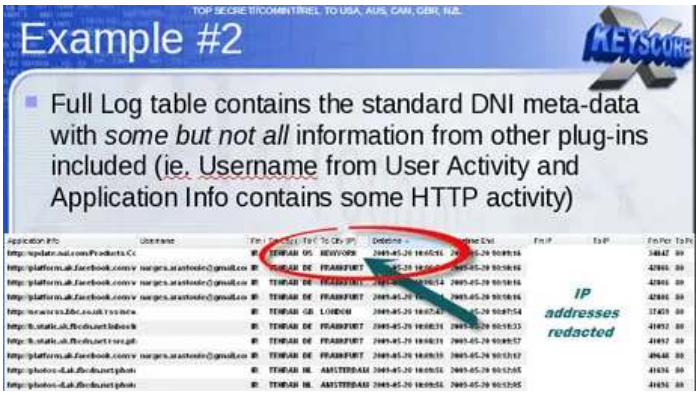
Legal v technical restrictions

While the Fisa Amendments Act of 2008 requires an individualized warrant for the targeting of US persons, NSA analysts are permitted to intercept the communications of such individuals without a warrant if they are in contact with one of the NSA's foreign targets.

The ACLU's deputy legal director, Jameel Jaffer, told the Guardian last month that national security officials expressly said that a primary purpose of the new law was to enable them to collect large amounts of Americans' communications without individualized warrants.

"The government doesn't need to 'target' Americans in order to collect huge volumes of their communications," said Jaffer. "The government inevitably sweeps up the communications of many Americans" when targeting foreign nationals for surveillance.

An example is provided by one XKeyscore document showing an NSA target in Tehran communicating with people in Frankfurt, Amsterdam and New York.



KS12 Photograph: Guardian

In recent years, the NSA has attempted to segregate exclusively domestic US communications in separate databases. But even NSA documents acknowledge that such efforts are imperfect, as even purely domestic communications can travel on foreign systems, and NSA tools are sometimes unable to identify the national origins of communications.

Moreover, all communications between Americans and someone on foreign soil are included in the same databases as foreign-to-foreign communications, making them readily searchable without warrants.

Some searches conducted by NSA analysts are periodically reviewed by their supervisors within the NSA. "It's very rare to be questioned on our searches," Snowden told the Guardian in June, "and even when we are, it's usually along the lines of: 'let's bulk up the justification'."

In a letter this week to senator Ron Wyden, director of national intelligence James Clapper acknowledged that NSA analysts have exceeded even legal limits as interpreted by the NSA in domestic surveillance.

Acknowledging what he called "a number of compliance problems", Clapper attributed them to "human error" or "highly sophisticated technology issues" rather than "bad faith".

However, Wyden said on the Senate floor on Tuesday: "These violations are more serious than those stated by the intelligence community, and are troubling."

In a statement to the Guardian, the NSA said: "NSA's activities are focused and specifically deployed against - and only against - legitimate foreign intelligence targets in response to requirements that our leaders need for information necessary to protect our nation and its interests.

"XKeyscore is used as a part of NSA's lawful foreign signals intelligence collection system.

"Allegations of widespread, unchecked analyst access to NSA collection data are simply not true. Access to XKeyscore, as well as all of NSA's analytic tools, is limited to only those personnel who require access for their assigned tasks ... In addition, there are multiple technical, manual and supervisory checks and balances within the system to prevent deliberate misuse from occurring."

"Every search by an NSA analyst is fully auditable, to ensure that they are proper and within the law.

"These types of programs allow us to collect the information that enables us to perform our missions successfully - to defend the nation and to protect US and allied troops abroad."

Topics

- The NSA files
- Glenn Greenwald on security and liberty
- Surveillance
- NSA
- Privacy
- Internet
- Data protection
- US politics
- news

UNCLASSIFIED//FOR OFFICIAL USE ONLY

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 6-20

Issue Date: 29 March 2014
Revised: 8 November 2016

(U) SECOND PARTY ACCESS TO NSA/CSS TS//SCI CLASSIFIED INFORMATION SYSTEMS

(U) PURPOSE AND SCOPE

(U) This policy defines processes and procedures for Second Party access to NSA/CSS classified information systems (IS). This policy applies to all United States Cryptologic System (USCS) organizations that sponsor Second Party personnel, NSA personnel who initiate or approve contracts for Second Party personnel access to U.S. classified intelligence and cryptographic information, and USCS personnel who implement Second Party personnel and systems access policy. NSA/CSS is lead for USA

RICHARD H. LEDGETT, JR.
Acting Director, NSA

Endorsed by
Associate Director for Policy

(U) Encl:
Annex - Second Party Access Information

(U) DISTRIBUTION:
T333
DC
D1 (Policy Records)
D3 (Authority)

(U) This Policy 6-20 supersedes NSA/CSS Policy 6-20 dated 2 July 2007
(U) OPI: NSA/CSS Threat Operations Center (NTOC), [redacted]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Policy 6-20 Dated: 31 March 2014

(U) This Policy 6-20 supersedes NSA/CSS Policy 6-20 dated 2 July 2012. The Chief, Policy approved an administrative update on 26 February 2015 to reflect new guidance on limited and minimal access agreements with Second Party integrees with NSA/CSS Policy 1-23, and take out-dated administrative clauses. The Chief, Policy approved an administrative update on 2 November 2015 to replace the definition "Authorizing Official." The Chief, Strategy, Plans, and Policy approved an administrative update on 8 November 2016 to restate applicability of Second Party Integrees and Liaison officers access to NSANet. The administrative update also added text to include "second party personnel" and "second party integrees" and makes distinctions between "second party personnel" and "second party integrees"; and makes minor corrections; improves accuracy in specifying NSANet access types; clarifies a Second Party and Multinational Affairs Division (P521) responsibilities; updates definitions; and makes minor administrative updates.

(U) POC: Technology Policy, P12, 2174(963).

(U) No portion of this document shall be released without approval from the Office of Policy (P12).

(U) POLICY

1. (U) It is the policy of NSA/CSS to share with Second Party Cryptologic partners all information relevant to the arrangements outlined in U.S. Signals Intelligence Directive 6 Agreement (U/~~FOUO~~) (Reference a) and subsequent bilateral memorandums with each Second Party nation as outlined in [redacted] (Reference b), NSA/GCHQ/DSD/CSE/GCSB "Second Party Intranet Connection MOU" (Reference c), and [redacted] (Reference d).

2. (U) Second Party systems connected to NSANet shall be operated in accordance with the requirements specified in the Director of National Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management" (Reference e).

3. (U//~~FOUO~~) Second Party Personnel may not perform information technology (IT) system administration functions or be granted privileged access on NSA/CSS IT systems, with the exception of limited administrative privileges in direct support of mission requirements (i.e., a virtual machine or workstation for administrative access to which is expressly required for mission purposes).

4. (U) Second Party system connections and access to any operational systems of the USG's Signals Intelligence enterprise and each Second Party must be established in a Memorandum of Understanding (MOU). Documents will be maintained and passed by Office of Policy (P12) on NSA/CSS Customer Relations SharePoint.

5. (U) Second Party integrees and Second Party Liaison officers who meet the access requirements in this policy shall routinely be granted user access to NSA/CSS classified systems at NSA/CSS premises.

6. (U) Second Party Accompanied Personnel shall not only access NSA/CSS classified ITs indirectly via the Second Party proxy server.

Policy 6-20 Dated: 31 March 2011

7. (U//~~FOUO~~) Second Party personnel who are not eligible for direct access and whose requirements cannot be accommodated via the proxy server may request an exception to obtain direct access to NSANet/SIPRNet via an individual NSANet account.

8. (U) All requests for Second Party personnel access to NSANet/SIPRNet shall be approved by the Second Party authority with responsibility to NSA/CSS mission or administrative information (e.g., system high or SIGINT Information Assurance [IA]), prior to submission to NSA/CSS for consideration. Second Party requests for individual NSANet accounts must be authorized in writing by the responsible Second Party authority.

9. (U) All Second Party personnel with access to classified NSANet/SIPRNet or in the performance of their SIGINT production mission must strictly follow the guidance within:

a. (U) SIGINT Directorate (SID) Management Directive 421, "United States SIGINT System Database Access" (Reference f),

b. (U) SID Management Directive 422, "USSS Mission Delegation" (Reference g), and

c. (U) SID Management Directive 427, "Access to Classified U.S. Intelligence Information for Second Party Personnel" (Reference h).

10. (U) For direct access to NSANet/SIPRNet classified IS, eligible Second Party personnel must be appropriately cleared and approved by the Second Party Liaison Officer Military Affairs Division (P522). In addition, Second Party personnel must be sponsored by a Global Enterprise Leader.

11. (U) All Second Party personnel who have obtained an NSANet user account shall complete NSA/CSS Information Assurance training (e.g., OVSC 1500, "Cyber Awareness Challenge," OVSC 1000, "Intelligence Oversight training") prior to access and yearly thereafter.

12. (U) All Second Party personnel with direct access to NSANet must obtain and use Cryptologic Agencies Domain certificates if possessing citizenship in a Five Eyes country. Additional information can be found on the NSA Corporate Public Key Infrastructure (PKI) Integration Page.

13. (U) All Second Party personnel with direct access to NSA/CSS IS shall be subject to all NSA/CSS Information Technology policies and procedures.

14. (U) The citizenship of all Second Party personnel given individual NSANet accounts shall be properly identified in the NSA/CSS Directory Service (e.g., SEARCHLIGHT) in order to provide automated network access control.

15. (U) Second Party personnel with individual NSANet accounts may be remotely connected only to those NSA/CSS classified IS required to perform sponsored functions. For foreigners, the sponsoring organization shall be the authority to identify what is required and shall

Policy 6-20 Dated: 31 March 2017

[illegible]

Issue 1 process to select on the systems and authentication accessed by the foreign [illegible] Gateway Client (NSTG) of all systems identified for Second Party integrees who may be updated to reflect exit access

15. (U//[illegible])

17. (U//[illegible])

18. (U//[illegible])

19. (U) All Second Party access to non-NSANet information on NSANet ISs shall be controlled in accordance with agreements with the information owners and processes established by the information owners and Accreditation Documentation. Non-NSANet information must be approved, in writing, by the originating organization of the data, as documented in the SSP.

20. (U) Under no circumstances will any Second Party Personnel to include positions, liaison officers or integrees be provided direct access to NSANet ISs. Such are used to generate, produce, or store/retrieve by manual and digital means U.S. only sensitive material, or Nuclear Command and Control Information Assurance Materials (NCCIAM).

21. (U) All Second Party personnel who no longer require access to NSANet ISs supplied ISs shall have their access terminated upon completion of work, not the official exit date. This process is non-transferable. If Second Party personnel require access in a new position, they will re-apply for the process based on their new duties.

(U) PROCEDURES

22. (U) Procedures for Second Party Indirect Access to NSANet Information Systems via Second Party Proxy Server.

a. (U) Written authorization is not required for Second Party personnel access to NSANet ISs via Second Party proxy servers; one

b. (U) Second Party personnel are not required to register with NSA/CSS before accessing NSA/CSS networks via Second Party provisioning.

27. (U) Procedures for Second Party Direct Access to NSA/CSS Information Systems. As noted above, Second Party liaison officers and integrees at NSA/CSS will be routinely sponsored for accounts at NSA/CSS. Other Second Party personnel may be approved for sponsorship on a case-by-case basis. The following procedures, therefore, apply to all Second Party liaison officers and integrees and to specially approved other Second Party personnel, as noted below. USCS organizations that wish to sponsor Second Party personnel for direct access to NSA/CSS IS shall:

a. (U) Complete and maintain, for each Second Party candidate, a record of the information specified within the Annex;

b. (U) For uniquely proposed, a formal requirements statement describing the system(s), information, and services required for the Second Party individual(s) to perform official NSA/CSS sanctioned duties; and

c. (U) Forward the sponsor and candidate information described in the above subparagraphs (and Annex) to the Second Party and Multinational Affairs Division (DS33) for approval and subsequent transmittal to the Office of Security and Counterintelligence (M5) for NSA/CSS Personnel Security System Database (e.g., CONCLAVE) record development. Approved Annexes will forward upon-on and end-state information through the secure two-way cryptographic channel (NSA/CSS Homeground).

28. (U) Exceptions to Access Policy: Organizations requesting an exception to this policy or its associated coordinate a written request with their Information System Security Officer (ISSO). Requests will be reviewed by the Information System Security Manager (ISSM) for Second Party and Multinational Affairs Division (DS33), prior to submission to the NSA/CSS Authorizing Official (AO) for decision.

(U) RESPONSIBILITIES

29. (U) USCS organizations sponsoring Second Party personnel for direct NSA/CSS IS access and NSA/CSS accounts shall:

a. (U) Verify the formal access requirements, to include need-to-know, for logon and services predefined for Second Party personnel and appropriately coordinated with other organizations when access to data from multiple information stewards is required;

b. (U) Serve as the sponsor-organization point-of-contact for Second Party personnel for [illegible] NSA/CSS-provided tools;

c. (U) Advise the Second Party and Multinational Affairs Division (P522) and Service Cryptologic Offices (if applicable) of the formal access request submitted by the Second Party or Multinational Affairs Division (P522) representative;

d. (U) Confirm that the sponsored Second Party personnel are registered in the NSA/CSS Personnel Security System Database (i.e., CONCERTO) and the NSA/CSS Directory service (i.e., SEARCHLIGHT);

e. (U) Verify that the Capabilities Directorate (Y) has approved all connectivity and access mechanisms before granting Second Party data access;

f. (U) Notify the Second Party and Multinational Affairs Division (P522), Service Cryptologic Offices (if applicable), the P522 Information Systems Security Manager (ISSM), the manager of the controlled interface, and system administrators when Second Party personnel access is no longer required;

g. (U) Be accountable for Second Party direct system access. Report any suspected anomalies, known or suspected unauthorized access, or problems associated with sponsored Second Party access in accordance with NSA/CSS Policy 6-26 "Reporting and Handling of NSA/CSS Information System Security Incidents" (Reference b); and

h. (U) Report anomalous activity and incidents to the Office of Security and Counterintelligence (Associate Capabilities Directorate (Y) for appropriate investigation.

24. (U) The Capabilities Directorate (Y) shall:

a. (U) Establish and maintain system accountability for Second Party access through the controlled interface and its appropriate services; and

b. (U) Provide technical guidance on security, technical risk assessment, and procedures for connecting any Second Party equipment to NSA/CSS classified networks.

27. (U) The Second Party or Multinational Affairs Division (P522) shall:

a. (U//~~FOUO~~) Ensure that sponsored NSA/CSS electronic systems such as Capabilities Directorate (Y) and the Office of Security and Counterintelligence (Q3) provide information on the activities and capabilities of Second Party persons sponsored for Direct NSA/CSS IS access/NSANet accounts. This will enable Standard Identification (sid) creation, SEARCHLIGHT record/account development/deletion as appropriate, and PKI approvals. These database records will form the core information set to enable NSA/CSS to satisfy internal, Department of Defense (DoD), Intelligence Community requirements for security and oversight of information access and exchange; and

h. (U//FOUO) Approve the creation of NSANET accounts for Second Party Personnel eligible for direct access.

20. (U) The Security and Counterintelligence (S&I) shall:

a. (U//FOUO) Receive and review approval requests from Second Party and Multinational (MN) Division (2S3) for Direct NSA/CSS IS access/NSANet accounts by Second Party persons and develop and maintain appropriate security records (e.g., CONCERTO) and conveyed and record data in Cryptohalities Directorate (V) records systems that support and mediate such access (e.g., S-ARK, HAWKEYE, CASPORT) process.

b. (U) Investigate any compromise or activity or incidents associated with Second Party access to NSA/CSS classified IS in coordination with the NSA/CSS Capabilities Directorate (V).

21. (U) The NSA/CSS Headquarters and Field ISSMs shall work with USCS organizations sponsoring Second Party integrees to ensure that information system security issues are addressed and resolved.

22. (U) NSA/CSS AO shall review requests for exceptions to this policy and render decisions.

23. (U) Privileged Access Users and ISSOs shall:

a. (U) Notify USCS system users when Second Party personnel have access to an IS or local area network:

b. (U//FOUO) Confirm that Second Party accounts are set up properly and removed upon completion of specified official duties per NSA/CSS Policy 6-5, "Information System User and Supervisor Security Responsibilities" (Reference h).

c. (U) Report any unusual activities in accordance with Reference k and assist, as necessary, in any investigations or analyses of such activities; and

d. (U) Assist in the enforcement of role-based access procedures established by the Information Assurance Component Enhancement Process.

(U) REFERENCES

24. (U) References:

a. (U) [U.S.-U.K. Communications Intelligence Agreement (UKUSA)] dated 5 March 1946.

b. (U) [redacted]

6

Policy 6-20 Issue: 31 March 2014

(U) References

a. (U) [redacted] (U) NSA/CSS/DoD/CSE/GCSB Second Party Internet Connection MOU dated 27 October 2005.

b. (U) [redacted]

c. (U) Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management," dated 21 July 2015.

d. (U) SID Management Directive (SMD) 421, "United States SIGINT System Database Access," revised 26 March 2008.

e. (U) SID Management Directive (SMD) 422, "USSS Mission Delegation," revised 17 April 2008.

f. (U) SID Management Directive (SMD) 427, "Access to Classified U.S. Intelligence Information for Second Party Personnel," revised 28 December 2009.

g. (U) SID Delegation of Approval Authorities Memo dated 20 November 2014.

h. (U) IAD Management Directive 128, "Approval and Release of Technical IA Information," dated 22 June 2012.

i. (U) NSA/CSS Policy 6-34, "Reporting and Handling of NSA/CSS Information Systems Security Incidents," dated 4 December 2013 and revised 14 November 2014.

j. (U) NSA/CSS Policy 6-6, "Information System User and Supervisor Security Responsibilities," dated 1 August 2016.

(U) DEFINITIONS

3a. (U) Authorizing Official (AO) – A senior (federal) official or executive with the authority to formally assume responsibility for operating a system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Source: CNSS Instruction (CNSSI) 4009 dated 6 April 2015.)

3d. (U) Cooperation – Related to cooperative efforts by entities of foreign governments and non-governmental entities (includes SIGINT, and solutions, products, and services to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of national security telecommunications and information systems (NSS) known as Information Assurance (IA). (Source: NSA/CSS Cryptologic Lexicon)

3f. (U) Exception – Indicates that an implementation of one or more security requirements is temporarily postponed and a plan and timetable for the requirement(s)

may be used for a specified period of time. This is in contrast to a waiver that implies a security requirement has been set aside and need not be implemented at all.

36. (U) Global Enterprise Leaders – NSA/CSS Director, the NSA Chief of Staff, SCC Commanders, Senior NSA/CSS Representatives, and the military commanders/civilian chiefs of NSA/CSS Extended Enterprises. (Source: NSA/CSS Capstone Policy Directive)

37. (U) Information System (IS) – Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition/collection, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice and/or data, and includes software, firmware, and hardware. Examples include: mainframes, minicomputers, Local Area Networks, servers, computers, process control computers that perform special purpose computing functions (e.g., Supervisory Control and Data Acquisition, other Industrial Control Systems, embedded computer systems), and telecommunications networks that disseminate information. (Source: NSA/CSS Corporate Policy Glossary)

38. (U) Information Steward – An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for generation, collection, processing, dissemination, and storage. (Derived from: CNSSI 4009)

39. (U) NSA/CSS Classified Network (NSANet) – The TS//SI information technology that enables the NSA/CSS to conduct its cryptologic missions including signals intelligence and information assurance and its cyber operations missions in concert with the NSA/CSS Global Cryptologic Enterprise. Several conditions must be satisfied for an IS to be considered part of the NSANet. In particular, each and every IS that is part of the NSANet must have a registered unique IP address; must be located in a SCIF [sensitive compartmented information facility] accredited by NSA/CSS or another IC agency or a Second Party Partner and approved by NSA/CSS or another NSA/CSS activity; and be under NSA/CSS authority. (Source: NSA/CSS Corporate Policy Glossary)

40. (U) NSA/CSS Washington (NSAW) – NSA/CSS facilities at the Fort Meade, Friendship Annex (FANX), and associated remote sites [Finksburg, Cheltenham, and all leased facilities in the Washington National Capital Region]. (Source: NSA/CSS Corporate Policy Glossary)

41. (U//~~FOUO~~) Nuclear Command and Control Materiel (NC2M) – Materiel used in safeguarding and controlling the use of nuclear weapons and weapon systems. These include, but are not limited to, materiels used in authentication, cryptography, and/or locking/unlocking functions associated with the command and control of nuclear weapons. (Source: NSA/CSS Corporate Policy Glossary)

42. (U) Privileged Access (PRIVACC) – A special access or set of special access rights required for performing data entry, file entry, operation of an application, or system. PRIVACC is granted to the following types of users:

a. (U) Users having "super user," "root," "administrator," or equivalent special access to a system (e.g., system administrator, computer system operations, system security officer, webmaster). These individuals have unrestricted access to the operating system of the machine or information system, or who set up and administer user accounts, authentications, and the like;

b. (U) Users who have been given the power to control or change other users access to data or programs (e.g., application or database owners, system-or specialty file owners, database managers, administrators);

c. (U) Users having access to change security parameters (e.g., passwords, password thresholds, violation actions, audit settings, and other system security parameters); and

d. (U) Users who have been granted special access for audit-related purposes in order to perform system security monitoring (Source: DIRNSA website ("the source")).

4. (U//~~FOUO~~) Second Party – refers to any of these countries: Australia, Canada, New Zealand, and the United Kingdom.

11. (U) Second Party Headquarters Personnel – Second Party personnel who work at Government Communications Headquarters (GCHQ), Communications Security Establishment (CSE), Australian Signals Directorate (ASD), or Government Communications Security Bureau (GCSB) headquarters or Technical Centre who have a valid need to access NSA/CSS facilities and for whom an NSA/CSS clearance is identified.

12. (U//~~FOUO~~) Second Party Integree – Second Party personnel integrated into an NSA/CSS or Central Security Service element who, when integrated into an NSA/CSS environment, are working solely under the direction and operational control of the DIRNSA/CHCSS to conduct cryptologic or information assurance activities that support the NSA/CSS mission in accordance with NSA/CSS authorities, roles, and regulations. Integrees may be a non-commissioned military Second Party SIGINT or IA professional but may not be a commissioned officer, or the Second Party cryptologic organization equivalent to warrant officer. NSA/CSS, under DIRNSA/CHCSS authorities. Duties associated with an Integree's position shall be performed in support of the NSA/CSS mission and in compliance with Executive Order 12333, "United States Intelligence Activities," as amended. (Source: NSA/CSS Corporate Policy Glossary)

13. (U) Second Party Liaison Officers – A government official from a Second Party country, either military or civilian, who works in support of his or her country's objectives at a US/Second Party organization or installation. These individuals generally act as the immediate point of contact for official interaction between DSD and the SP for their geographic location. (Source: Working definition, DOD and 5 Eyes Partner Fact Sheet, June 5, 2013)

47. (U) Service Partners – Those organizations with the Service armed services that operate under Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) authority, or joint members of the larger Unified Cryptologic System, but that are not part of the CSS (e.g., Army Cyber Division, Squadron Brigade and Armed Cavalry Regiment, or Navy Fleet SIGINT Readiness Officer) normally under SIGINT Operational Tasking Authority (SOTA) of a tactical commander. (Reference j)

48. (U) System Security Plan (SSP) – The SSP is a document prepared by the information system owner (or common security control owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configuration management plan, and incident response plan. (Source: CNSSI 4009)

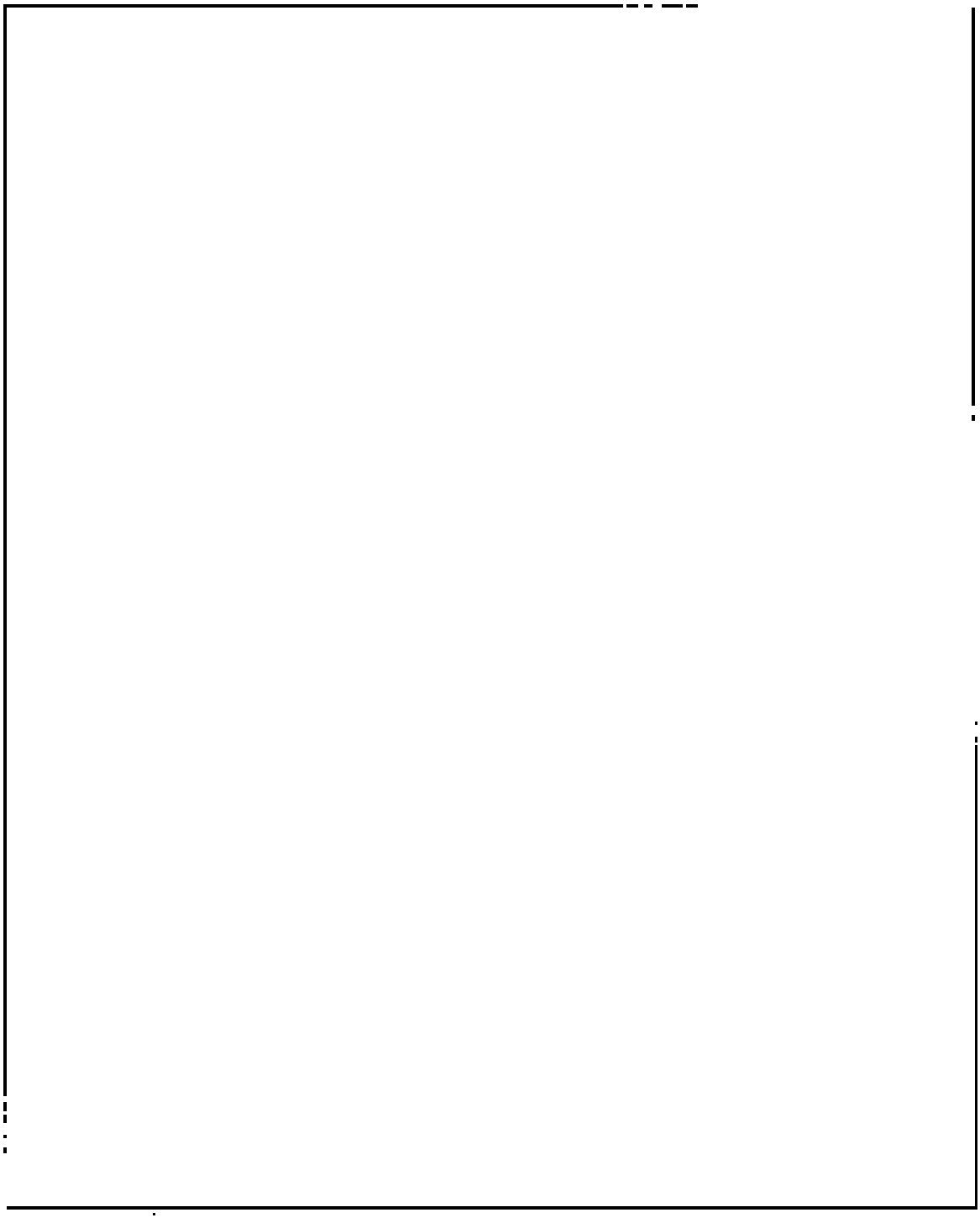
49. (U) United States Cryptologic System (USCS) – The whole of the U.S. Government cryptologic activity, including SIGINT mission, i.e., the collection, processing, and dissemination of SIGINT, or with an information assurance mission, i.e., preserving the availability, integrity, authentication, confidentiality, and nonrepudiation of national security telecommunications and information systems. (Source: NSA/CSS Corporate Policy Glossary)

50. (U) USCS Personnel – United States Government personnel who derive their authority to direct and conduct cryptologic operations (SIGINT and IA) from the Director, NSA/Chief, CSS (DIRNSA/CHCSS). CSCS Government personnel can be defined in three categories:

a. (U) Civilian employees of the National Security Agency.

b. (U) Military personnel and service civilians of the Service Cryptologic Components.

c. (U) Military personnel and service civilians of the non-CSS military organizations and civilian integrees from other U.S. intelligence community agencies who are considered as members of the USCS when performing SIGINT or IA operations under the direction, authority, and control of DIRNSA/CHCSS. (Source: NSA/CSS Corporate Policy Glossary)



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 1-13

Date: [illegible]
Reissued

(U) SECOND PARTY INTEGREES

(U) PURPOSE AND SCOPE

(U//FOUO) This policy assigns responsibilities and procedures for the [illegible] of [illegible] Second Party integrees, including [illegible] NSA/CSS. This policy applies to [illegible] NSA/CSS [illegible], and United States Signals Intelligence System [illegible].

MICHAEL S. ROGERS
Admiral, U.S. Navy
Director, NSA/Chief, CSS

Endorsed by
Associate Director for Policy

(U) DISTRIBUTION:
[illegible]
DJ

[redacted] Effective [redacted]

(U) This Policy 1.7 supersedes NSACSS Policy 1.7 dated 6 January 2001
(U) OPI: Program Affairs Directorate, Public Policy [redacted]
(U) No waivers to this document may be granted without prior approval from the Director, National Cryptologic School.

(U) POLICY

1. (U//FOUO) [redacted] NSACSS shall support the training and education needs of [redacted] personnel from the Key NSACSS Partners by [redacted] NSACSS Signals Intelligence Directorate objectives as specified in the United States Cryptologic Strategy, the National Intelligence Priorities Framework, and guidance from the Director of National Intelligence, the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Director, National Security Agency/Chief, Central Security Service. This training and education shall be consistent with requirements for safeguarding [redacted] and the protection of intelligence sources and methods.

2. (U//FOUO) [redacted] National Cryptologic School (NCS) is assigned responsibility for the following functions: [redacted] NSACSS Associate Directorates, and Key Partners, as well as other organizations as determined by the Signals Intelligence Directorate, including [redacted] NSACSS activities, to take actions which will enhance cryptologic support to mission personnel, operations, and intelligence production. Specific responsibilities are detailed in the Responsibilities section of this policy. Such actions will be consistent with the Cryptologic Training Strategy and will be coordinated with all appropriate organizations. Unless otherwise specified, National Cryptologic School activities will be conducted in accordance with NSACSS Directive [redacted] and applicable regulatory guidance.

3. (U//FOUO) [redacted] National Cryptologic School may use [redacted] information to determine [redacted] personnel who are eligible to attend [redacted] courses at NCS. [redacted] will be consistent with the principles of need-to-know, minimum necessary, and limited use. [redacted] information will be used only for the purposes for which it was collected. [redacted] information will be protected from unauthorized disclosure, [redacted] Information Assurance Directorate (IAD), Publication 6001, Marking Technology Systems, and Key Management Plan, as amended. [redacted] Policy 1-52, NSACSS Policy 1-52, dated [redacted] Information [redacted] will be released outside NSACSS only [redacted] National Cryptologic School Privacy Act Officer, [redacted] Public Affairs Directorate, [redacted] Exceptions to this paragraph must be approved and endorsed by the Information Protection Security Officer (IPSO) prior to submission to the NSACSS Authorizing Official for review.

c. (U//FOUO) Second Party Integrees may be assigned to leadership positions; however, any supervisory responsibilities for the oversight of any U.S. [illegible] officer or employee of the U.S. Government must be performed by the next higher-level U.S. supervisor in the integrated chain of command. This means that the Second Party Integree leader must properly forward administrative documents, including but not limited to performance evaluations, awards, pay [illegible], making decisions regarding the employee's [illegible] or similar personnel actions for any integrated NSA/CSS employee. Second Party Integrees may, however, provide input to U.S. Government leaders' official appraisals [illegible]. Additionally, [illegible] Second Party Integree [illegible] position [illegible] the specific details and scope of an [illegible] duties.

9. (U//FOUO) Information necessary for Second Party Integrees to perform their [illegible] qualified by [illegible] NSA/CSS, Director of National Intelligence (DNI), DoD, Committee on National Security Systems (CNSS) policy, applicable Executive Orders, or U.S. law. [illegible] associated with Second Party Integrees must be coordinated [illegible] Second Party Integree [illegible]

10. (U) Organizations wishing to establish and staff new Second Party Integree positions shall follow the procedures detailed below.

(U) PROCEDURES

11. (U//FOUO) Requirements for Second Party Integree positions will be identified within NSA/CSS Directorates, Associate Directorates, the NSA/CSS Chief of Staff organization, or NSA/CSS Extended Enterprise elements. This policy provides a formal [illegible] between NSA/CSS and Second Party organizations to identify and define these requirements.

12. (U//FOUO) The sponsoring organization seeking to establish, extend, or terminate an integrated position will prepare, coordinate, and formally submit the necessary documentation through the Foreign Affairs Office of the Signals Intelligence (SIGINT) Operations Group (SOG), Foreign Affairs Directorate (FAD), and the Associate Directorate for Security and Counterintelligence (ADS&CI) to the appropriate Director, Deputy Director, Associate Director, or NSA/CSS Chief of Staff [illegible] governing [illegible] review and approval. For SID the approval [illegible] in accordance with the SID Delegation of Approval Authorities [illegible]. The approved package will be returned to FAD for final review and coordination [illegible] subsequent [illegible] of the position.

13. (U//FOUO) The appropriate Director, Associate Director, the NSA/CSS Chief of Staff or their designee may approve exceptions to this policy when necessary to effect rapid realignment of Second Party Integree resources in response to urgent mission requirements.

2. (U) [illegible] Second Party Integree position [illegible]

a. (U//FOUO) NSA/CSS [illegible] Second Party Integree position [illegible] mission and associated [illegible] New NSA/CSS [illegible] Intelligence [illegible] in accordance with the [illegible] Intelligence Community [illegible] NSA/CSS [illegible] [redacted] In addition, a Non-Disclosure Agreement (NDA) shall be executed with the Second Party Integree before release of any PROPIN data.

b. (U//FOUO) [illegible] required for a Second Party Integree [illegible] NSA/CSS [illegible] Second Party Integree [illegible]

c. (U//FOUO) Second Party personnel [illegible] NSA/CSS sponsored training are exempt from this policy. However, if access to NSA/CSS networks is [illegible] training, Second Party personnel shall adhere to NSA/CSS Policy [illegible]

d. (U//FOUO) Security considerations regarding [illegible] Second Party Integree [illegible] requirements shall be [illegible] subject to a DSCI [illegible] compliance with information systems, physical and personnel security [illegible] before establishing or staffing any position.

e. (U//FOUO) [illegible] Second Party Integree position [illegible] requirements that shall be [illegible] coordinated with the appropriate NSA/CSS offices. New Second Party Integree positions or Second Party Integree [illegible] approved [illegible] Second Party Integree [illegible] shall be coordinated through [illegible] Second Party Integree [illegible] developmental programs (e.g., Cryptologic Mathematician Program, Language Analyst [illegible] Program, etc.) [illegible] Second Party Integree [illegible] All appropriate approvals and applicable documentation must be obtained at least 30 days prior to [illegible]

if approved, to the maximum extent possible, prior to the Second Party Integree beginning the new extended assignment.

9. (U//FOUO) In cases where a Second Party Integree will perform duties at or visit any U.S. Government contractor, the U.S. Government contractor will be required to comply with U.S. laws and regulations, including those governing exports (e.g., the Arms Export Control Act and the International Traffic in Arms Regulations (ITAR), 22 CFR 120-130 (Reference h)). The Office of Export Control Policy (DJ7) is the Agency's authority for export licensing. DJ7 identifies the licenses required for contractors to interact with Second Party Integrees (Reference g).

10. (U) The Office of the General Counsel will address any questions regarding whether the integration of Second Party personnel into the NSA/CSS workforce or Second Party use of NSA/CSS capabilities is consistent with U.S. law and regulations that govern NSA/CSS activities.

(U) RESPONSIBILITIES

11. (U//FOUO) Directors, Associate Directors, the NSA/CSS Chief of Staff, and the Extended Enterprise Commanders/Chiefs shall:

a. (U//FOUO) Identify requirements for Second Party Integree positions at specific assignments, extensions, and reassignments within their respective organizations;

b. (U//FOUO) Document Second Party Integree requirements for the Second Party Affiliate Office (SPAO). The documentation should include the following:

1) (U//FOUO) A justification explaining why each requirement for Second Party Integree position is necessary or beneficial to advance the U.S. cryptologic mission or the Second Party relationship;

2) (U//FOUO) A description of the specific duties the Second Party Integree will be performing;

3) (U) Affirmation that the level of intelligence and information assurance sharing is consistent with current operational requirements and a statement of the [illegible] security clearance required for the position;

(U//FOUO) 4) A statement of [illegible] requirements [illegible] [redacted] [illegible] SIGINT data [illegible] SID will follow SID Management Directive [illegible] "Access to Data for Second Party Integrees [illegible] in SIGINT Production" (Reference h).

5. (U//~~FOUO~~) A description of the security procedures that will be instituted within the Integree's assigned element to prevent the unauthorized disclosure of NOFORN information, information that is releasable to a community other than the Second Party Integree's own (for example, REL US/UK information for a Canadian Integree), and [illegible] information subject to NSA/CSS Special Access Requirements and [illegible] approval has been granted per paragraph 13.

6. (U//~~FOUO~~) Agreement regarding [illegible] will be made available to the Second Party Integree's nation. Such decisions will be managed with the organization to which the Integree is assigned and in accordance with procedures in place to ensure the proper and authorized release of NOFORN.

7. (U) Requirements for annual training needed by the Second Party Integree, including mandatory intelligence oversight training, other training required of personnel working under DIRNSA/CHCSS SIGINT authority, or National Cryptologic School courses.

8. (U//~~FOUO~~) Assurance that the Second Party parent organization (through its national Senior Liaison Office) [illegible] and provide guidance for the assigned Second Party Integree personnel, in coordination with FAD, ADS&CI, and the involved OPI(s).

9. (U//~~FOUO~~) [redacted]

(b) (3)-P.L. 86-36

10. (U//~~FOUO~~) An acknowledgment of specific obligations [illegible] regarding the Integree's [illegible] management needs. The parent organization accepts responsibility for [illegible] will [illegible] evaluation [illegible] the Integree [illegible].

a. (U//~~FOUO~~) [illegible]

b. (U//~~FOUO~~) [illegible]

e. (U//FOUO) Coordinate with ADS&CI, the Foreign Affairs Directorate, and the relevant Oversight and Compliance organizations to [illegible] security responsibilities for integrating Second Party personnel into classified operational elements.

f. (U//FOUO) Review the qualifications of and approve or disapprove candidates who are nominated to fill Second Party Integree positions. Forward Second Party Integree selections and [illegible] to the Second Party Affairs Office [illegible].

(b)(3)-P.L. 86-36 [illegible] (U//FOUO) [redacted]

g. (U//FOUO) Coordinate with the Information Assurance Directorate (IAD) when a Second Party Integree has been [illegible] (IA) approved requirement for access to United States Information Security data, including, but not limited to, incident and vulnerability information, U.S. cryptographic algorithms, IA techniques, and U.S. computer security information.

h. (U//FOUO) Coordinate with the appropriate Information Systems Security Officer and/or Information Systems Security Manager to ensure appropriate security certification and accreditation documents, risk assessments, and security controls are in place [illegible] when the Second Party Integree [illegible] access to a U.S. information system, in accordance with NSA/CSS Policy [illegible] "Second Party Access to NSA/CSS TS/SCI Classified Information Systems" (Reference [illegible]).

i. (U//FOUO) Advise the DIRNSA Second Party Affairs Office of any proposed changes in the status of Second Party Integree positions, including position extensions and the replacement of Integrees, [illegible] in advance of the proposed change when it is possible.

12. (U) The Foreign Affairs Directorate shall:

a. (U//FOUO) Review all requests for establishing new or [illegible] Second Party Integree positions (SPIP) to ensure they are consistent and in compliance with existing policy and procedures;

b. (U//FOUO) Coordinate with Second Party Liaison Offices to identify Second Party Integree positions and the personnel that fill them;

c. (U//FOUO) Maintain a record of all approved positions and dates nominated for all Second Party Integree positions [illegible]. [illegible] approval [illegible] appropriate.

d. (U) Notify the affected Second Party Liaison Office of any decisions.

the approvals of Second Party Integree positions.

e. (U//~~FOUO~~) Advise appropriate organizations when all necessary administrative, security, and personnel actions have been completed so that access to [illegible] granted to the Second Party Integree;

f. (U//~~FOUO~~) Maintain a current, comprehensive list of all Second Party Integrees at NSAW and the Extended Enterprise, including names, assigned organizations, and length of tour; and

g. (U//~~FOUO~~) Ensure that the Second Party partner organizations, through their Senior [illegible] Liaison Office or [illegible], send adequate certification and relevant background information on proposed Integrees (name, date and place of birth, date of last security clearance and investigation, citizenship, [illegible]) [illegible] the Integree's home agency.

15. (U) The Associate Director for Security and Counterintelligence shall:

a. (U//~~FOUO~~) Review and assess the personnel and physical security [illegible] Second Party personnel [illegible] specific NSA/CSS operational elements [illegible], provide recommendations [illegible];

b. (U//~~FOUO~~) Establish [illegible] security records for each Second Party Integree, consisting of basic identification, clearance certification, status, and [illegible] background investigations and [illegible] from the Integree's home agency;

c. (U//~~FOUO~~) Verify and maintain appropriate [illegible] clearance and eligibility for access information for all Second Party Integrees;

d. (U) [illegible] and control records of NSA/CSS [illegible] information [illegible] to Second Party Integrees in accordance with Reference [illegible]; and

e. (U) Issue each Second Party Integree the appropriate [illegible] badge required for access to NSA/CSS [illegible] buildings in accordance with NSA/CSS Policy [illegible], "NSA/CSS Badge [illegible]" (Reference [illegible]).

16. (U) The Technology Directorate, as the NSA/CSS Chief Information Officer, and the NSA/CSS Chief Information Security Officer (CISO) shall:

a. (U//~~FOUO~~) Review and assess the information systems security ramifications of integrating or assigning Second Party personnel [illegible] NSA/CSS operational element locations;

1. [illegible] implements applicable policy and assigns responsibilities in accordance with the authorities of DoD Directive [illegible], "Inspector General of the Department of Defense," August 7, 2012, DoD Instruction 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012, and DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 26, 2013.

2. [illegible] the assessment and management of risks associated with information technology that exports digital [illegible] Department Approved Products [illegible] to Second Party customers, and the appropriate certification, evaluation, and validation of cryptographic capability for the NSA-CSS Type 1 Cryptographic [illegible].

II. RESPONSIBILITIES

A. IG DoD

1. [illegible] Publications.

2. [illegible] "National Maintenance of Foreign Materiel," dated 22 June 2010.

3. [illegible] "Information Technology Systems Security Risk Management, Certification and Accreditation," dated 28 September 2007, as amended.

4. [illegible] "Cybersecurity," dated 14 March 2014.

5. [illegible] "Information Technology Security Certification and Accreditation Activities," dated 3 March 2014.

6. [illegible] "Secret and Below Interoperability (SABI) and Top Secret SCI Interoperability (TSABI/TSI)," dated 3 March 2014.

7. [illegible] 32 CFR 236-150.5 and DoD Instruction [illegible], "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," dated 21 November 2014.

8. [illegible] "Cyber Incident Reporting," dated 31 December 2014.

9. [illegible] "Secure Configuration Management," dated 3 December 2014.

10. [illegible] "Information Assurance Workforce Improvement Program," dated 19 December 2005, as amended.

11. [illegible] "Cybersecurity Workforce Management and Qualification," dated 12 February 2015.

12. [illegible] "Cybersecurity," dated 23 March 2011, as amended.

Policy [illegible] Date: [illegible] Determination [illegible]

(U) DEFINITIONS

(U//FOUO) Controlled Information. SOFCOS and associated information [illegible] is controlled unclassified information [illegible] Examples include [illegible]

(U//FOUO) Non-DoD Controlled Unclassified Information. NSA personnel are authorized to receive, [illegible]

a. (U) NSA/CSS Employee. Defined as all full time, part time or contractor personnel [illegible]

b. (U) NSA/CSS Workforce (NSA/CSSW). NSA/CSS civilian employees [illegible] and assigned military personnel [illegible]

c. (U) Associates. Selected non-NSA/CSS personnel [illegible] and who have been granted access to [illegible]

(U//FOUO) Foreign Partner. Any [illegible] U.S. Government [illegible] Australia, Canada, the United Kingdom, Canada, Australia, and New Zealand.

(U) Second Party Integree. Second Party personnel assigned to NSA/CSS in a United States Cryptologic [illegible] and who have been granted access to NSA/CSS information systems under the terms and specific limitations of the [illegible] NSA/CSS Integree Instruction with NSA/CSS authorities, access, and duties. Integrees may be assigned to the NSA/CSS Second Party [illegible] and who have been granted access to [illegible] Executive Order 12333, "United States Intelligence Activities," as amended [illegible]

(U//FOUO) Second Party Liaison. [illegible] representing the [illegible] Second Party [illegible] NSA/CSS [illegible] and who have been granted access to NSA/CSS. Duties associated with this position [illegible]

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND

NSA/CSS DIR NO. 90-3
DATE: 25 November 1990

NSA/CSS DIRECTIVE

SECOND PARTY INTEGREES (U)

SECTION

SECTION I - PURPOSE AND APPLICABILITY

1. This directive establishes policy, assigns responsibilities and prescribes procedures for the establishment of Second Party integrees positions within the NSA/CSS. This directive is applicable to all cryptologic elements and facilities located within CONUS or overseas and includes those sites or facilities operated/manned either directly by the NSA/CSS or the Service Cryptologic Elements (SCEs).

SECTION II - DEFINITIONS

2. Second Party: That term applies either individually or collectively to the following nations with whom the NSA/CSS maintains special SIGINT and Information exchange relationships:

- The United Kingdom
- Canada
- Australia
- New Zealand

3. Second Party Integree Position: A position established by NSA/CSS (to include CCPO or overseas cryptologic facilities) which will be filled on a permanent change of station (PCS)

basis by an individual representing one of the Second Party nations. Duties associated with this position will be performed in furtherance of the mission of NSA/CSS.

SECTION III - POLICY

4. The integration of Second Party personnel into the NSA/CSS work force is supported when it is beneficial to the U.S. SIGINT or INFOSEC mission, or its SIGINT or INFOSEC relationships with the Second Party Nations identified in paragraph 2., above.

5. Security ramifications to include possible exposure to special operations or compartments, NOFORN, industrial proprietary or any other information not releasable to Second Parties, must be considered prior to the establishment and staffing of any Second Party integree positions.

6. All requirements for Second Party integrees will be fully coordinated with appropriate Second Party SIGINT or INFOSEC authorities and approved by the affected Key Component Chief for the Chief of a COMSEC or overseas cryptologic site or facility prior to the establishment and staffing of the proposed positions.

7. Second Party integrees will not be placed in positions in which they have a direct effect upon the NSA/CSS decision-making process, to include both contractual and policy deliberations. Under no circumstances should they be placed in positions whereby they are solely responsible for addressing such issues, nor represent Agency interests in external meetings or conferences.

8. The processing, staffing and assignment of Second Party personnel to COMSEC or overseas cryptologic sites or facilities will be handled in the same manner as Second Party personnel integrated into NSA/CSS Headquarters elements.

9. The temporary assignment of Second Party personnel for on-the-job or classroom training (for a period not to exceed six months) is not subject to the processing and approval requirements of this Directive. Host organizations, however, must ensure that security and administrative steps are taken to preclude inadvertent disclosure of U.S. or NSA/CSS-only information for the duration of the training period.

SECTION IV. - RESPONSIBILITIES

10. The Chiefs of Key Components and Chiefs of COMSEC or overseas cryptologic sites or facilities will:

a. Identify requirements for Second Party integree positions and assignments within their respective organizations.

b. Prepare written documentation of Second Party integree requirements. This documentation will include the following information:

(1) A justification as to why the establishment of the position is necessary or important to either the U.S. SIGINT or Information mission or the Second Party relationship.

(2) A description of the specific duties the Second Party integree will be performing.

(3) The specific procedures that will be instituted within the assigned organization to preclude the inadvertent disclosure of U.S.-only information or Special Activities Programs.

c. Coordinate with the Deputy Director for Operations (DDO), Special Activities Office (DDO/SAO) regarding special access requirements, and with the Deputy Director for Administration (DDA), Security (M5), to assess any special security considerations, e.g. key control, lock installations, access control to ADP systems, etc., that may be needed to provide adequate safeguards to preclude the inadvertent disclosure of sensitive U.S.-only information or other proprietary entities.

d. Forward Second Party integree position requests to the Deputy Director for Plans and Policy (DDPP) for review (verification of conformance with existing policy) and approval.

e. Review the qualifications of and approve candidates who are nominated to fill Second Party integree positions.

f. Advise the DDPP of any changes in the status of Second Party integree positions to include rotation and replacement of specific personnel.

q. Establish procedures for the non-disclosure of proprietary or "commercial-in-confidence" information which is received during an integree's tenure.

r. Coordinate with the NSA/CSS SCSM (Senior Computer Security Manager) and the Information Systems Security International Relations, Policy and Doctrine Organization (S11) when an integree or trainee has a requirement for access to U.S. Information Systems Security information, including but not limited to IPC/SIGINT threat and vulnerability information, U.S. cryptographic algorithms or INFOSEC technologies, or U.S. computer security information.

11. The Deputy Director for Plans and Policy (DDPP) will:

a. Review and approve all requests for establishment of Second Party integree positions to verify and ensure conformance of the requests with existing policy.

b. Coordinate with the Second Party liaison offices to staff these positions.

c. Solicit the approval of requesting organizations for candidates nominated to fill Second Party integree positions.

d. Maintain a record of all Second Party integrees to include names, assigned elements, length of tour, etc. (Q32).

e. Obtain, from the Second Party parent organization, a certification of the clearances/accesses of proposed integrees, as well as relevant background information on the proposed integree (to include at a minimum name, date and place of birth, date of last security background investigation or reinvestigation, citizenship, and citizenship of spouse). The Office of Foreign Relations (Q3) will provide this information to X2 and Y09/Z40 and will advise these organizations of any changes in the status of integrees which would affect their clearances/access certifications.

12. The Deputy Director for Administration (DDA) will:

a. Provide advice and assistance regarding physical and personnel security policies and procedures as they may relate to integrating Second Party personnel into specific NSA/CSS organizations in CONUS or overseas.

b. Establish and maintain a data base of clearance and security background information initially provided and kept current by Q4 for all Second Party integrees.

c. Review security background data provided by Q4 on nominated Second Party integrees, and provide endorsements to Q4 prior to Agency acceptance of the integrees for assignment.

13. The Deputy Director for Operations (DDO) will administer and maintain records of accesses to NSA/CSS special access programs by all Second Party integrees (DOS/SAO).

14. The Deputy Director for Telecommunication and Computer Services, (DDT), under the auspices of the Office of Operational Computer Security (V09), will:

a. Review and assess the computer security ramifications of integrating Second Party personnel into specific NSA/CSS positions.

b. Provide, in accordance with the requirements of DCID 1/16 (Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks), computer security guidance to organizations requesting Second Party access to NSA/CSS computer systems or networks.

SECTION V - PROCEDURES

15. Requirements for Second Party integrees will be identified within the operational elements of the Key Components or COMSEC or overseas cryptologic sites or facilities. This regulation does not preclude informal exchanges between NSA/CSS and Second Party operational elements for purposes of identifying and defining those requirements.

16. The operational element wishing to establish an integrated position will prepare and forward the necessary paperwork to their Key Component Chief (or Chief of COMSEC or overseas cryptologic site or facility) for review and approval.

17. The Chiefs of Key Components or Chiefs of COMSEC or overseas cryptologic sites or facilities will review, approve and forward Second Party integree requirements to the Deputy Director for Plans and Policy.

NSA/CSS DIRECTIVE NO. 21-3

18. Q3, in coordination with the Office of Policy (Q4), will perform necessary policy reviews and prepare an appropriate recommendation for the DUPR.

19. Subject to DCID endorsement, Q3 will coordinate with the Second Party liaison offices to begin the staffing process.

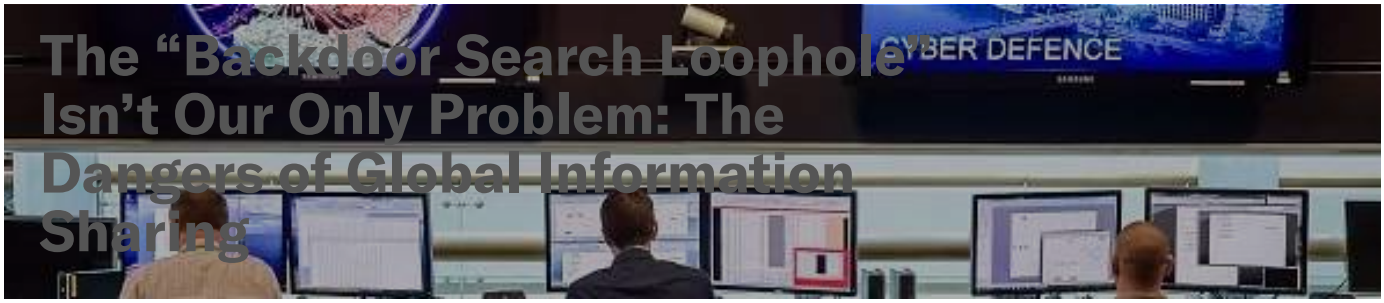
20. Q3 will advise the requesting organization of candidates nominated to fill Second Party integree positions and reporting dates and solicit their approval to proceed with follow-on staffing actions.

21. Q3, upon approval of the Key Component Chief or the Chief of a CCNUS or overseas cryptologic site or facility, will advise M5 and P05/SAO of the individual selected to fill a Second Party integreed position. This will ensure that all necessary administrative, security and personnel actions are adequately addressed prior to the arrival of that individual.

W. O. STUDEMAN
Vice Admiral, U.S. Navy
Director

DISTRIBUTION: I

Plus: Q13 (20 copies)
Q14 (20 copies)
P05 (VHB)



The “Backdoor Search Loophole” Isn’t Our Only Problem: The Dangers of Global Information Sharing

by Scarlet Kim, Paulina Perlin and Diana Lee

November 28, 2017

The upcoming expiration of Section 702 of the Foreign Intelligence Surveillance Act (FISA) has launched a fresh wave of debate on how the statute’s “backdoor search loophole” allows the U.S. government to access Americans’ communications by searching information gathered on foreign intelligence grounds without a warrant. But while discussion about domestic information sharing is important, a critical element of the debate is missing: the privacy risks posed by *global* information sharing between the United States and foreign powers. Like its domestic analog, global information sharing may also permit the U.S. government to access and search Americans’ data without appropriately accommodating their constitutional rights.

The U.S. is party to a number of international information-sharing arrangements—the most prominent being the Five Eyes alliance. Born from spying arrangements forged during World War II, the Five Eyes alliance facilitates the sharing of signals intelligence among the U.S., the United Kingdom, Australia, Canada, and New Zealand. These sharing arrangements are memorialized in the United Kingdom-United States Communication Intelligence (UKUSA) Agreement.

Still, little is known about the legal frameworks governing intelligence sharing among the Five Eyes. The UKUSA Agreement has been amended several times, but the most recent publicly available version dates back to 1955. That version of the agreement indicates that the Five Eyes are to share, by default, the “products” of “operations relating to foreign communications,” as well as the methods and

techniques relating to such operations. An appendix to the agreement further indicates that the Five Eyes are to share “continuously, currently, and without request” both “raw” (i.e. unanalyzed) “traffic” in addition to analyzed “end product.”

Our limited understanding of how intelligence sharing might operate, particularly in the digital era, is informed by the U.S. government’s intelligence programs under Section 702. Through “Upstream” surveillance, the NSA undertakes bulk interception of Americans’ international communications, including emails and web-browsing content, as they transit the cables, switches, and routers that constitute the internet “backbone.” The NSA then searches these communications using tens of thousands of “selectors,” or keywords. Media reports have revealed that the NSA has access to a U.K. bulk surveillance program similar to “Upstream,” which intercepts internet traffic as it flows through the undersea cables landing in the U.K. We do not know the extent to which the U.K. intelligence agencies have similar access to information stored within Section 702-derived databases. However, media reports have revealed that the Five Eyes (as well as other foreign partners) have access to databases storing information collected through various NSA programs, including MARINA, a metadata repository, and XKEYSCORE, which uses hundreds of servers around the world to store information acquired under various NSA programs.

Privacy Implications

Intelligence sharing raises significant privacy concerns. Technological advances have dramatically changed both communication methods and signals intelligence capabilities since 1955. The development of new technology, especially the internet, has transformed the way we communicate with each other and increased the amount of information that can be collected by orders of magnitude. As our communications have evolved, intelligence agencies have developed more advanced ways to acquire, store, analyze, and share this information. They can intercept in bulk communications and data transiting the internet. Computers

permit revelatory analyses of types and amounts of data that were previously considered meaningless or incoherent. And the internet has facilitated remote access to information, easing sharing between agencies.

Critics of Section 702 note that the NSA’s intelligence operations targeting foreigners could sweep in millions of Americans’ private communications. It is possible that under the UKUSA Agreement, the NSA both shares this information with foreign governments and receives U.S. persons’ communications that foreign agencies collect. It is not clear, for example, how the Five Eyes exchange raw signals intelligence intercepted in bulk—“continuously, currently, and without request”—while constraining access to the data of their respective citizens.

The scarcity of information about the Five Eyes alliance compounds these privacy concerns. The U.S. government has not explained how the UKUSA Agreement currently operates, the types of information that the U.S. government accesses, or the rules that constrain U.S. intelligence agencies’ access to and dissemination of Americans’ private communications.

This lack of transparency weakens the oversight and accountability mechanisms available to check global intelligence sharing. Absent additional information regarding the UKUSA Agreement and Five Eyes alliance, Americans must rely on a 60-year-old, likely outdated, document; veiled government statements; and media reports to understand how their privacy might be implicated by foreign intelligence practices. Adding to this concern is that while the Five Eyes alliance is the best known intelligence sharing arrangement, the U.S. is also party to many more.

Privacy International, together with Yale Law School’s Media Freedom & Information Access Clinic, is currently pursuing litigation under the Freedom of Information Act to obtain the updated text of the UKUSA Agreement and its minimization procedures. To date, however, the NSA, the agency primarily responsible for signals intelligence, has not yet disclosed any responsive records. (A

similar request to the U.K.’s Government Communications Headquarters (GCHQ)—the British signals intelligence agency—was denied on grounds that GCHQ is entirely exempt from the U.K.’s freedom of information framework.)

Privacy advocates concerned about Section 702 should therefore broaden their attention to the privacy risks inherent in global information sharing. The U.S. government should make available the text of the current version of the UKUSA Agreement, as well as related implementing procedures. It should also make public subsequent revisions to the UKUSA Agreement and other agreements governing intelligence sharing with foreign parties. And to the extent that these documents reveal that the U.S. government receives Americans’ information without appropriate procedural safeguards, lawmakers should demand additional privacy protective restrictions.

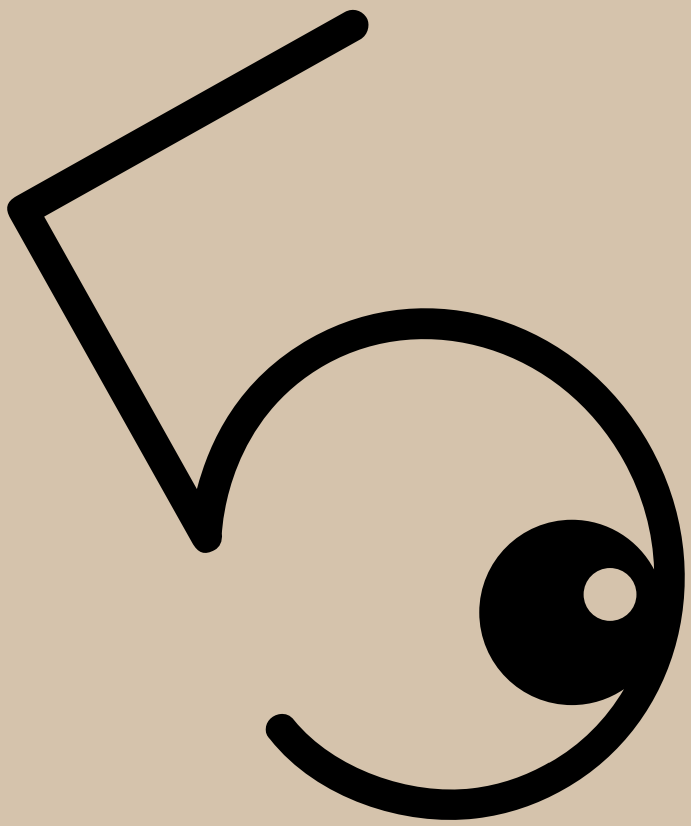
As Congress turns its attention to Section 702, we should not ignore the privacy risks posed by longstanding international intelligence sharing practices that proposed domestic reforms will not touch. Without more information about the legal underpinnings of these agreements, and how they operate in practice, we cannot adequately protect the privacy of Americans and foreigners alike.

Image: Getty

PRIVACY INTERNATIONAL

Eyes Wide Open

Special Report



Executive Summary

The recent revelations, made possible by NSA-whistleblower Edward Snowden, of the reach and scope of global surveillance practices have prompted a fundamental re-examination of the role of intelligence services in conducting coordinated cross-border surveillance.

The Five Eyes alliance of States – comprised of the United States National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Canada's Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB) – is the continuation of an intelligence partnership formed in the aftermath of the Second World War. Today, the Five Eyes has infiltrated every aspect of modern global communications systems.

The world has changed dramatically since the 1940s; then, private documents were stored in filing cabinets under lock and key, and months could pass without one having the need or luxury of making an international phone call. Now, private documents are stored in unknown data centers around the world, international communications are conducted daily, and our lives are lived – ideas exchanged, financial transactions conducted, intimate moments shared – online.

The drastic changes to how we use technology to communicate have not gone unnoticed by the Five Eyes alliance. A leaked NSA strategy document, shared amongst Five Eyes partners, exposes the clear interest that intelligence agencies have in collecting and analyzing signals intelligence (SIGINT) in the digital age:

> "Digital information created since 2006 grew tenfold, reaching 1.8 exabytes in 2011, a trend projected to continue; ubiquitous computing is fundamentally changing how people interact as individuals become untethered from information sources and their communications tools; and the traces individuals leave when they interact with the global network will define the capacity to locate, characterize and understand entities."[1]

Contrary to the complaints of the NSA and other Five Eyes agencies that they are 'going dark' and losing the visibility they once had, the Five Eyes intelligence agencies are in fact the most powerful they've ever been. Operating in the shadows and misleading the public, the agencies boast in secret how they "have adapted in innovative and creative ways that have led some to describe the current day as 'the golden age of SIGINT'."

The agencies are playing a dirty game; not content with following the already permissive legal processes under which they operate, they've found ways to infiltrate all aspects of

[1] NSA SIGINT Strategy, 23 February 2012, available at: http://www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html?ref=politics&gwh=5E154810A5FB56B3E9AF98DF667AE3C8

modern communications networks. Forcing companies to handover their customers' data under secret orders, and secretly tapping fibre optic cables between the same companies' data centers anyway. Accessing sensitive financial data through SWIFT, the world's financial messaging system, spending years negotiating an international agreement to regulate access to the data through a democratic and accountable process, and then hacking the networks to get direct access. Threatening politicians with trumped up threats of impending cyber-war while operating intrusion operations that weaken the security of networks globally; sabotaging encryption standards and standards bodies thereby undermining the ability of internet users to secure information.

Each of these actions have been justified in secret, on the basis of secret interpretations of international law and classified agreements. By remaining in the shadows, our intelligence agencies – and the governments who control them – have removed our ability to challenge their actions and their impact upon our human rights. We cannot hold our governments accountable when their actions are obfuscated through secret deals and covert legal frameworks. Secret law has never been law, and we cannot allow our intelligence agencies to justify their activities on the basis of it.

We must move towards an understanding of global surveillance practices as fundamentally opposed to the rule of law and to the well-established international human right to privacy. In doing so, we must break down legal frameworks that obscure the activities of the intelligence agencies or that preference the citizens or residents of Five Eyes countries over the global internet population. These governments have carefully constructed legal frameworks that provide differing levels of protections for internal versus external communications, or those relating to nationals versus non-nationals, attempt to circumvent national constitutional or human rights protections governing interferences with the right to privacy of communications.

This notion must be rejected. The Five Eyes agencies are seeking not only defeat the spirit and purpose of international human rights instruments; they are in direct violation of their obligations under such instruments. Human rights obligations apply to all individuals subject to a State's jurisdiction. The obligation to respect privacy extends to the privacy of all communications, so that the physical location of the individual may be in a different jurisdiction to that where the interference with the right occurs.

This paper calls for a renewed understanding of the obligations of Five Eyes States with respect to the right to privacy, and demands that the laws and regulations that enable intelligence gathering and sharing under the Five Eyes alliance be brought into the light.

It begins, in **Chapter One**, by shining a light on the history and structure of the alliance, and draws on information disclosed by whistleblowers and investigative journalists to paint a picture of the alliance as it operates today. In **Chapter Two**, we argue that the laws and regulations around which Five Eyes are constructed are insufficiently clear and accessible to ensure they are in compliance with the rule of law. In **Chapter Three**, we turn to the obligations of Five Eyes States under international human rights law and argue for an "interference-based jurisdiction" whereby Five Eyes States owe a general duty not to interfere with communications that pass through their territorial borders. Through such a conceptualization, we argue, mass surveillance is cognisable within a

human rights framework in a way that provides rights and remedies to affected individuals.

While the existence of the Five Eyes has been kept secret from the public and parliaments, dogged investigative reporting from Duncan Campbell, Nicky Hager, and James Bamford has gone some way to uncovering the extent of the arrangement. Now, thanks to Edward Snowden, the public are able to understand more about the spying that is being done in their name than ever before.

Trust must be restored, and our intelligence agencies must be brought under the rule of law. Transparency around and accountability for these secret agreements is a crucial first step.

Privacy International to grateful is Ben Jaffey, Caspar Bowden, Dan Squires, Duncan Campbell, Eric Metcalfe, Ian Brown, James Bamford, Mark Scott, Marko Milanovic, Mathias Vermeulen, Nicky Hager, Shamik Dutta, for their insight, feedback, discussions, investigation and support. We are grateful to all of the whistleblowers whose responsible disclosures in the public interest have brought transparency to the gross violations of human rights being conducted by the intelligence agencies in our name.

Given the current rapid nature of information disclosures regarding the intelligence agencies, this paper will be regularly updated to reflect the most accurate understanding we have of the nature of the Five Eyes arrangement. Any errors or omission are solely attributable to the authors.

Version 1.0 – 26 November 2013

Chapter 1 – Understanding the Five Eyes

The birth of the Five Eyes alliance

Beginning in 1946, an alliance of five countries (the US, the UK, Australia, Canada and New Zealand) developed a series of bilateral agreements over more than a decade that became known as the UKUSA (pronounced yew-kew-zah) agreement, establishing the Five Eyes alliance for the purpose of sharing intelligence, but primarily signals intelligence (hereafter "SIGINT"). While the existence of the agreement has been noted in history books and references are often made to it as part of reporting on the intelligence agencies, there is little knowledge or understanding outside the services themselves of exactly what the arrangement comprises.

Even within the governments of the respective countries, which the intelligence agencies are meant to serve, there has historically been little appreciation for the extent of the arrangement. The arrangement is so secretive the Australian Prime Minister reportedly wasn't informed of its existence until 1973[2]. Former Prime Minister of New Zealand, David Lange, once remarked that "it was not until I read this book [Nicky Hager's "Secret Power", which detailed GCSB's history] that I had any idea that we had been committed to an international integrated electronic network." He continued: "it is an outrage that I and other ministers were told so little, and this raises the question of to whom those concerned saw themselves ultimately answerable."[3]

There has been no debate around the legitimacy or purpose of the Five Eyes alliance in part due to the lack of publicly available information about it. In 2010, the US and UK declassified numerous documents, including memoranda and draft texts, relating to the creation of the UKUSA agreement. However, generally the Five Eyes States and their intelligence services have been far too slow in declassifying information that no longer needs to be secret, resulting in no mention on any government website of the arrangement until recently.

The intelligence agencies involved in the alliance are the United States National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Canada's Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB).

The extent of the original arrangement is broad and includes the

(1) collection of traffic;
(2) acquisition of communications documents and equipment;

[2] Canada's role in secret intelligence alliance Five Eyes, CTV News, 8 October 2013, available at: http://knlive.ctvnews.ca/mobile/the-knlive-hub/canada-s-role-in-secret-intelligence-alliance-five-eyes-1.1489170
[3] Secret Power, Nicky Hager, 1996, page 8 available at: http://www.nickyhager.info/Secret_Power.pdf

(3) traffic analysis;
(4) cryptanalysis;
(5) decryption and translation; and
(6) acquisition of information regarding communications organizations, procedures, practices and equipment.

A draft of the original UKUSA agreement, declassified in 2010, explains that the exchange of the above-listed information

> "will be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon."

Indeed, in addition to facilitating collaboration, the agreement suggests that all intercepted material would be shared between Five Eyes States by default. The text stipulates that "all raw traffic shall continue to be exchanged except in cases where one or the other party agrees to forgo its copy."

The working arrangement that was reached in 1953 by UKUSA parties explained that "while Commonwealth countries other than the UK are not party to the UKUSA COMINT agreement, they will not be regarded as Third Parties."[4] Instead "Canada, Australia and New Zealand will be regarded as UKUSA-collaborating Commonwealth countries," also known as Second Parties. One retired senior NATO intelligence officer has suggested "there is no formal over-arching international agreement that governs all Five Eyes intelligence relationships."[5] It is not known how accurate that statement is, or how the agreement has been modified in subsequent years as the text of the Five Eyes agreement in its current form has never been made public.

Today, GCHQ simply states it has "partnerships with a range of allies […] [o]ur collaboration with the USA, known as UKUSA, delivers enormous benefits to both nations."[6] The NSA makes no direct reference to the UKUSA arrangement or the Five Eyes States by name, except by way of historical references to partnerships with "the British and the Dominions of Canada, Australia, and New Zealand" in the declassification section of their website.[7]

The original agreement mandated secrecy, stating "it will be contrary to this agreement to reveal its existence to any third party unless otherwise agreed" resulting in modern day references to the existence of the agreement by the intelligence agencies remaining

---

[4] Appendix J, Principles of UKUSA collaboration with commonwealth countries other than the UK. Page 39, available at: http://www.nationalarchives.gov.uk/ukusa/
[5] Canada and the Five Eyes Intelligence Community, James Cox, Strategic Studies Working Group Papers, December 2012, page 4, accessible at: http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf
[6] International Partners, GCHQ website, available at: http://www.gchq.gov.uk/how_we_work/partnerships/Pages/International-partners.aspx
[7] UKUSA Agreement Release 1940-1956, NSA website, available at: http://www.nsa.gov/public_info/declass/ukusa.shtml

limited. The existence of the agreement was not acknowledged publicly until March 1999, when the Australian government confirmed that the Defence Signals Directorate (now Australian Signals Directorate) "does co-operate with counterpart signals intelligence organisations overseas under the UKUSA relationship."[8]

Canada's CSEC[9] states it maintains intelligence relationships with NSA, GCHQ, ASD and GCSB, but only New Zealand's GCSB[10] and ASD[11] mention the UKUSA agreement by name.[12]

This obfuscation continues, with only cursory mentions made across a wide range of public policy documents to the existence of an intelligence sharing partnership. For example the UK Counter-Terrorist Strategy CONTEST, referred to the existence of the Five Eyes agreement only in passing when stating the UK will "continue to develop our most significant bilateral intelligence relationship with the US, and the 'Five Eyes' cooperation with the US, Australia, Canada and New Zealand."[13]

We have been unable to locate any major public strategic policy document that describes Australia's, Canada's, New Zealand's or the United States' involvement in the Five Eyes in any detail.

The extent of Five Eyes collaboration

The close relationship between the five States is evidenced by documents recently released by Edward Snowden. Almost all of the documents include the classification "TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL" or "TOP SECRET//COMINT//REL TO USA, FVEY." These classification markings indicate the material is top-secret communications intelligence (aka SIGINT) material that can be

[8] The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition, October 1999, page 1, available at: http://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf

[9] CSEC's International Partnerships, CSEC website, available at: http://www.cse-cst.gc.ca/home-accueil/about-apropos/peers-homologues-eng.html

[10] UKUSA Allies, GCSB website, available at: http://www.gcsb.govt.nz/about-us/UKUSA.html

[11] UKUSA Allies, ASD website, available at: http://www.asd.gov.au/partners/allies.htm

[12] The New Zealand Prime Minister, John Key, has specifically referred to "Five Eyes" on several occasions; at his 29 October 2013 press conference, for example, in answer to the question, 'Do you think the GCSB was aware of the extent of spying from the NSA on foreign leaders?" he replied: "Well I don't know all of the information they exchanged, the discussions they had with their counterparts. They are part of Five Eyes so they had discussions which are at a much more granular level than I have….", audio available at: http://www.scoop.co.nz/stories/HL1310/S00224/pms-press-conference-audio-meridian-spying-and-fonterra.htm. Similarly, at his 25 October, press conference, with reference to Edward Snowden, he stated "He has a massive amount of data, we're part of Five Eyes, it's highly likely he's got information related to New Zealand", video available at http://www.3news.co.nz/Snowden-highly-likely-to-have-spy-info/tabid/1607/articleID/322789/Default.aspx#ixzz2lgdCec1l.

[13] Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, HM Government, 2010, page 46, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf

released to the US, Australia, Canada, United Kingdom and New Zealand. The purpose of the REL TO is to identify classified information that a party has predetermined to be releasable (or has already been released) through established foreign disclosure procedures and channels, to a foreign country or international organisation.[14] Notably while other alliances and coalitions exist such as the North Atlantic Treaty Organisation (e.g. TS//REL TO USA, NATO), European Counter-Terrorism Forces (e.g TS//REL TO USA, ECTF) or Chemical Weapons Convention States (e.g. TS//REL TO USA, CWCS) none of the documents that have thus far been made public refer to any of these arrangements, suggesting the Five Eyes alliance is the preeminent SIGINT collection alliance.

The arrangement in this way was not just to create a set of principles of collaboration, or the facilitation of information sharing, but to enable the dividing of tasks between SIGINT agencies. The agreement explains that

> "[a]llocation of major tasks, conferring a one-sided responsibility, is undesirable and impracticable as a main principle; however, in order that the widest possible cover of foreign cypher communications be achieved the COMINT agencies of the two parties shall exchange proposals for the elimination of duplication. In addition, collaboration between those agencies will take the form of suggestion and mutual arrangement as to the undertaking of new tasks and changes in status of old tasks."[15]

The continuation of this sharing of tasks between agencies has been acknowledged with former Defense Secretary Caspar Weinberger observing that the "United States has neither the opportunity nor the resources to unilaterally collect all the intelligence information we require. We compensate with a variety of intelligence sharing arrangements with other nations in the world."[16] The Canadian SIGINT agency CSEC explain how it "relies on its closest foreign intelligence allies, the US, UK, Australia and New Zealand to share the collection burden and the resulting intelligence yield."[17] Other former intelligence analysts have confirmed[18] there is "task-sharing" between the Five Eyes groups.

---

[14] Security Classification Markings—Authorization for ReleaseTo (RELTO)and Dissemination Control/ Declassification Markings, USTRANSCOM Foreign Disclosure Office, available at: http://www.transcom.mil/publications/showPublication.cfm?docID=04A4D891-1EC9-F26D-0715CB3E5AF1309B

[15] Appendix E, Co-ordination of, and exchange of information on, cryptanalysis and associated techniques. page 34, available at: http://www.nationalarchives.gov.uk/ukusa/PDF page 34

[16] Declaration of the Secretary of Defence Caspar W Weinberger in USA v Jonathan Pollard, 1986. Available at: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB407/docs/EBB-PollardDoc6.pdf

[17] Safeguarding Canada's security through information superiority, CSEC website, available at: http://www.cse-cst.gc.ca/home-accueil/media/information-eng.html

[18] Britain's GCHQ 'the brains,' America's NSA 'the money' behind spy alliance, Japan Times, 18th November, 2013, accessible at: http://www.japantimes.co.jp/news/2013/11/18/world/britains-gchq-the-brains-americas-nsa-the-money-behind-spy-alliance/#.UozmbMvTnqB

The level of co-operation under the UKUSA agreement is so complete that "the national product is often indistinguishable."[19] This has resulted in former intelligence officials explaining that the close-knit cooperation that exists under the UKUSA agreement means "that SIGINT customers in both capitals seldom know which country generated either the access or the product itself."[20] Another former British spy has said that "[c]ooperation between the two countries, particularly, in SIGINT, is so close that it becomes very difficult to know who is doing what [...] it's just organizational mess."[21]

The division of SIGINT collection responsibilities

Investigative journalist Duncan Campbell explains that historically

> "[u]nder the UKUSA agreement, the five main English-speaking countries took responsibility for overseeing surveillance in different parts of the globe. Britain's zone included Africa and Europe, east to the Ural Mountains of the former USSR; Canada covered northern latitudes and polar regions; Australia covered Oceania. The agreement prescribed common procedures, targets, equipment and methods that the SIGINT agencies would use."[22]

More recently an ex-senior NATO intelligence officer elaborated on this point, saying

> "[e]ach Five Eyes partner collects information over a specific area of the globe […] but their collection and analysis activities are orchestrated to the point that they essentially act as one. Precise assignments are not publicly known, but research indicates that Australia monitors South and East Asia emissions. New Zealand covers the South Pacific and Southeast Asia. The UK devotes attention to Europe and Western Russia, while the US monitors the Caribbean, China, Russia, the Middle East and Africa."[23]

Jointly run operations centres

In addition to fluidly sharing collected SIGINT, it is understood that many intelligence facilities run by the respective Five Eyes countries are jointly operated, even jointly staffed, by members of the intelligence agencies of Five Eyes countries. Each facility

---

[19] Robert Aldrich (2006) paper 'Transatlantic Intelligence and security co-operation', available at: http://www2.warwick.ac.uk/fac/soc/pais/people/aldrich/publications/inta80_4_08_aldrich.pdfIntelligence'
[20] S. Lander, 'International intelligence cooperation: an inside perspective', in Cambridge Review of International Affairs, 2007, vol. 17, n°3, p.487.
[21] Britain's GCHQ 'the brains,' America's NSA 'the money' behind spy alliance, Japan Times, 18th November, 2013, accessible at: http://www.japantimes.co.jp/news/2013/11/18/world/britains-gchq-the-brains-americas-nsa-the-money-behind-spy-alliance/#.UozmbMvTnqB
[22] Inside Echelon, Duncan Campbell, 2000, available at: http://www.heise.de/tp/artikel/6/6929/1.html
[23] Canada and the Five Eyes Intelligence Community, James Cox, Strategic Studies Working Group Papers, December 2012, accessible at: http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf page 6

collects SIGINT, which can then be shared with the other Five Eyes States.

An earlier incarnation of ASD, the Defence Signals Branch in Melbourne,[24] was described in the original 1956 UKUSA agreement as

> "not purely a national centre. It is and will continue to be a joint U.K – Australian – New Zealand organization manned by and 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 the London Signal Intelligence Board on the other. On technical matters control is exercised by GCHQ on behalf of the London Signal Intelligence Board."

This jointly run operation has continued, with the Australian Joint Defence Facility at Pine Gap being staffed by both Australian and US intelligence officers. The facility collects intelligence that is jointly used and analysed.[25] In fact, only half of the staff are Australian,[26] with US intelligence operatives from NSA and other agencies likely accounting for the rest. An American official runs the base itself, with the posting being considered "a step towards promotion into the most senior ranks of the US intelligence community" with an Australian acts as deputy.[27] With such an overwhelming US presence, it is likely that that majority of the cost of running is base is paid for by the US; the Australian Defence Department says Australia's contribution to Pine Gap's in 2011-12 was a mere AUS$14 million.[28]

The systems run at the base are tied into the largest Five Eyes intelligence structure with "personnel sitting in airconditioned offices in central Australia [being] directly linked, on a minute-by-minute basis, to US and allied military operations in Afghanistan and indeed anywhere else across the eastern hemisphere."[29] As a result it has been reported that "[t]he practical reality is that Pine Gap's capabilities are now deeply and inextricably entwined with US military operations, down to the tactical level, across half the world."[30] The New Zealand GCSB was similarly entwined with the NSA: the GCSB's Director of

---

[24] See: "The Defence Signals Bureau was established in 1947, as part of the Department of Defence, with responsibility for maintaining a national sigint capability in peacetime. In 1977, DSD assumed its current name" available at: http://www.dpmc.gov.au/publications/intelligence_inquiry/chapter7/4_dsd.htm

[25] Pine Gap drives US drone kills, The Age, 21st July 2013, available at: http://www.smh.com.au/national/pine-gap-drives-us-drone-kills-20130720-2qbsa.html

[26] Australian outback station at forefront of US spying arsenal, The Sydney Morning Herald, 26th July 2013, available at: http://www.smh.com.au/it-pro/security-it/australian-outback-station-at-forefront-of-us-spying-arsenal-20130726-hv10h.html

[27] Australian outback station at forefront of US spying arsenal, The Sydney Morning Herald, 26th July 2013, available at: http://www.smh.com.au/it-pro/security-it/australian-outback-station-at-forefront-of-us-spying-arsenal-20130726-hv10h.html

[28] Pine Gap drives US drone kills, The Age, 21st July 2013, available at: http://www.smh.com.au/national/pine-gap-drives-us-drone-kills-20130720-2qbsa.html

[29] Pine Gap drives US drone kills, The Age, 21st July 2013, available at: http://www.smh.com.au/national/pine-gap-drives-us-drone-kills-20130720-2qbsa.html

[30] Australian outback station at forefront of US spying arsenal, The Sydney Morning Herald, 26th July 2013, available at: http://www.smh.com.au/it-pro/security-it/australian-outback-station-at-forefront-of-us-spying-arsenal-20130726-hv10h.html

Policy and Plans from 1984-1987, for example, was an NSA employee.[31]

In addition to bases in Australia and New Zealand, Britain's history of Empire left GCHQ with a widespread network of SIGINT outposts. Intelligence stations in Bermuda, Cyprus, Gibraltar, Singapore and Hong Kong have all played critical collection roles over the past 60 years.

One of the largest listening posts outside the US is based in northern England, yet has been under US ownership since the 1950s. In 1996 the base was renamed RAF Menwith Hill and it was reported that for the first time the Union Jack was raised alongside the Stars and Stripes. David Bowe, MEP for Cleveland and Richmond, said this was "designed to mislead" and that "[m]y information is that the RAF representation on the base amounts to one token squadron leader. The name change was presumably decided to make the whole site look more benign and acceptable."[32] The base was the subject of a six billion pound investment over last 20 years, with the majority of that likely to be US funds.[33]

Other bases, such as GCHQ's operation in the South West of England at Bude, are also jointly staffed. The Guardian reported[34] that in addition to jointly developing the TEMPORA program, 300 analysts from GCHQ and 250 from the NSA were located at Bude and directly assigned to examine material collected under the programme.

In his seminal report *Interception Capabilities 2000*, Duncan Campbell named a number of foreign or jointly run NSA bases. He wrote

> "[t]he US Air Force installed 500 metre wide arrays known as FLR-9 at sites including Chicksands, England, San Vito dei Normanni in Italy, Karamursel in Turkey, the Philippines, and at Misawa, Japan. Codenamed "Iron Horse", the first FLR-9 stations came into operation in 1964. The US Navy established similar bases in the US and at Rota, Spain, Bremerhaven, Germany, Edzell, Scotland, Guam, and later in Puerto Rico, targeted on Cuba."[35]

---

[31] A fact unknown to the Prime Minister at the time: Hager, Secret Power, p. 21.
[32] US spy base `taps UK phones for MI5', The Independant, 22 September 1996, available at: http://www.independent.co.uk/news/uk/home-news/us-spy-base-taps-uk-phones-for-mi5-1364399.html
[33] US spy base `taps UK phones for MI5', The Independant, 22 September 1996, available at: http://www.independent.co.uk/news/uk/home-news/us-spy-base-taps-uk-phones-for-mi5-1364399.html
[34] An early version of TEMPORA is referred to as the Cheltenham Processing Centre, additionally codenamed TINT, and is described as a "joint GCHQ/NSA research initiative". The Guardian quotes an internal GCHQ report that claims "GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures." It was additionally reported that NSA provided GCHQ with the technology necessary to sift through the material collected. The Guardian reported that 300 analysts from GCHQ and 250 from NSA were directly assigned to examine the collected material, although the number is now no doubt much larger. GCHQ have had staff examining collected material since the project's incarnation in 2008, with NSA analysts brought to trials in Summer 2011. Full access was provided to NSA by Autumn 2011. An additional 850,000 NSA employees and US private contractors with top secret clearance reportedly also have access to GCHQ databases
[35] Inside Echelon, Duncan Campbell, 2000, available at: http://www.heise.de/tp/artikel/6/6929/1.html

Many of these sites remain active, as an NSA presentation displaying the primary foreign collection operations bases shows. The presentation[36] details both the US sites distributed around the world as well as the 2nd party bases as follows:

Type	Location	Country	Codename
US site	Yakima	US	JACKNIFE
US site	Sugar Grove	US	TIMBERLINE
US site	Sabana Seca	Puerto Rico	CORALINE
US site	Brasillia	Brasil	SCS
US site	Harrogate (aka Menwith Hill)	UK	MOONPENNY
US site	Bad Aibling[37]	Germany	GARLICK
US site	New Delhi	India	SCS
US site	Thailand	Thailand	LEMONWOOD
US site	Misawa[38]	Japan	LADYLOVE
2nd Party	Bude	UK	CARBOY
2nd Party	Oman	Oman	SNICK
2nd Party	Nairobi	Kenya	SCAPEL
2nd Party	Geraldton	Australia	STELLAR
2nd Party	Cyprus	Cyprus	SOUNDER
2nd Party	New Zealand	New Zealand	IRONSAN

It is important to note that, just because a base is being operated from within a particular country, this does not forestall Five Eyes parties from collecting intelligence therein on the host country. Ex-NSA staff have confirmed that communications are monitored from "almost every nation in the world, including the nations on whose soil the intercept bases are located."[39]

Intelligence collection, analysis and sharing activities

It is believed that much of the intelligence collected under the Five Eyes arrangement can be accessed by any of the Five Eyes partners at any time. Some codenamed programmes that have been revealed to the public over the last decade go some way to illustrating how the Five Eyes alliance collaborates on specific programmes of activity and how some of this information is shared. It should be noted that these are just a selection of programmes that have been made public, and are likely to represent a tiny fraction of the joint collection undertaken by Five Eyes partners. Nevertheless these codenamed programmes reveal just how integrated the Five Eyes SIGINT collection and analysis methods are, and the existence of shared SIGINT tools and technologies

[36] New slides about NSA collection programs, Electrospaces blog, 16th July, 2013, available at: http://electrospaces.blogspot.co.uk/2013/07/new-slides-about-nsa-collection-programs.html
[37] Bad Aibling Station, Wikipedia, available at: http://en.wikipedia.org/wiki/Bad_Aibling_Station
[38] http://www.misawa.af.mil/ and http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/docs/doc12.pdf
[39] Inside Echelon, Duncan Campbell, 2000, available at: http://www.heise.de/tp/artikel/6/6929/1.html

themselves.

As early as the 1980s, Five Eyes countries used a "global Internet-like communication network to enable remote intelligence customers to task computers at each collection site, and receive the results automatically."[40] This network was known as ECHELON and was revealed to the public in 1988 by Duncan Campbell.[41] An often-misunderstood term, ECHELON is in fact a

> "code name given by the NSA (U.S. National Security Agency) to a system that collects and processes information derived from intercepting civil satellite communications. The information obtained at ECHELON stations is fed into the global communications network operated jointly by the SIGINT organisations of the United States, United Kingdom, Australia, Canada and New Zealand. ECHELON stations operate automatically. Most of the information that is selected is automatically fed into the world-wide network of SIGINT stations."[42]

It is not known how long the ECHELON programme continued in that form, but the NSA went on to develop programmes such as THINTHREAD, which emerged at the turn of the millennium. THINTHREAD was a sophisticated SIGINT analysis tool used "to create graphs showing relationships and patterns that could tell analysts which targets they should look at and which calls should be listened to."[43] One of the creators of THINTHREAD, Bill Binney described the tool to the New Yorker:

> "As Binney imagined it, ThinThread would correlate data from financial transactions, travel records, Web searches, G.P.S. equipment, and any other "attributes" that an analyst might find useful in pinpointing "the bad guys." By 2000, Binney, using fibre optics, had set up a computer network that could chart relationships among people in real time. It also turned the N.S.A.'s data-collection paradigm upside down. Instead of vacuuming up information around the world and then sending it all back to headquarters for analysis, ThinThread processed information as it was collected – discarding useless information on the spot and avoiding the overload problem that plagued centralized systems. Binney says, "The beauty of it is that it was open-ended, so it could keep expanding."[44]

This programme was distributed around the world and trialed in conjunction with the Five Eyes partners. Tim Shorrock explains:

> "The THINTHREAD prototype went live in the fall of 2000 and […] several allied foreign intelligence agencies were given the programme to conduct lawful

---

[40] Inside Echelon, Duncan Campbell, 2000, available at: http://www.heise.de/tp/artikel/6/6929/1.html
[41] Somebody's listening, New Statesmen, 12 August 1988, available at: http://web.archive.org/web/20070103071501/http://duncan.gn.apc.org/echelon-dc.htm
[42] http://www.duncancampbell.org/menu/surveillance/echelon/IC2001-Paper1.pdf, page 2.
[43] US spy device 'tested on NZ public', The New Zealand Herald, 25th May 2013, available at: http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10886031
[44] The Secret Sharer, The New Yorker, 23 May 2011, available at: http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all

> surveillance in their own corners of the world. Those recipients included Canada, […] Britain, Australia and New Zealand."[45]

Analysis tools such as these have been developed in secret over many years, often at huge cost. That this tool was shared, even in trial version with Five Eyes partners, is an important indicator of how tightly integrated the relationship is. Subsequent related programmes codenamed TRAILBLAZER, TURBULENCE and TRAFFICTHIEF were later adopted and used by Five Eyes partners.[46]

More recently, the Guardian reported[47] that 300 analysts from GCHQ and 250 from the NSA were directly assigned to examine material collected under the TEMPORA programme. By placing taps at key undersea fibre optic cable landing stations, the programme is able to intercept a significant portion of the communications that traverses the UK. TEMPORA stores content for three days and metadata for 30 days. Once content and data are collected, they can be filtered.

The precise nature of GCHQ's filters remains secret. Filters could be applied based on type of traffic (e.g. Skype, Facebook, Email), origin/destination of traffic, or to conduct basic keyword searches, among many other purposes. Reportedly, approximately 40,000 search terms have been chosen and applied by GCHQ, and another 31,000 by the NSA to information collected via TEMPORA.

GCHQ have had staff examining collected material since the project's inception in 2008, with NSA analysts brought to trial runs of the technology in summer 2011. Full access was provided to NSA by autumn 2011. An additional 850,000 NSA employees and US private contractors with top-secret clearance reportedly also have access to GCHQ databases. GCHQ boasted that it had "given the NSA 36% of all the raw information the British had intercepted from computers the agency was monitoring."[48] Additional reporting from GCHQ internal documents explains how they "can now interchange 100% of GCHQ End Point Projects with NSA."[49]

GCHQ received £100 million ($160 million) in secret NSA funding over the last three years to assist in the running of this project. This relationship was characterized by Sir David Omand, former Director of GCHQ, as "a collaboration that's worked very well […] [w]e have the brains; they have the money."[50]

---

[45] http://motherboard.vice.com/blog/the-nsa-reportedly-tested-its-top-spyware-on-new-zealand
[46] http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html
[47] An early version of TEMPORA is referred to as the Cheltenham Processing Centre, additionally codenamed TINT, and is described as a "joint GCHQ/NSA research initiative". The Guardian quotes an internal GCHQ report that claims "GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures." It was additionally reported that NSA provided GCHQ with the technology necessary to sift through the material collected.
[48] http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance
[49] GCHQ: Inside the top secret world of Britain's biggest spy agency, The Guardian, 2 August 2013, available at http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden
[50] http://www.japantimes.co.jp/news/2013/11/18/world/britains-gchq-the-brains-americas-nsa-the-money-behind-spy-alliance/

Liaison officers are charged with the ultimate responsibility of ensuring continued harmony and cooperation between their agencies and as James Bamford, author or multiple books on the NSA explains "it is the senior liaison officers, the SIGINT community's version of ambassadors, who control the day-to-day relations between the UKUSA partners. And it is for that reason that the post of SUSLO (Office of the Senior United States Liaison Officer) at NSA is both highly prized and carefully considered."[51] These positions to facilitate co-operation continue to exist throughout the arrangement. A recent diplomatic cable from the US Ambassador in Wellington, New Zealand, released by WikiLeaks, noting that "[t]he National Security Agency (NSA) has requested a new, permanent position in Wellington."[52] The cable went on to state:

> "The new position will advance US interests in New Zealand by improving liaison and cooperation on vital signals intelligence matters. This is an area where the US and NZ already work together closely and profitably, and continuing to build and expand that relationship clearly stands to benefit both countries. This is especially true in the post-September 11 environment, where NZ SIGINT capabilities significantly enhance our common efforts to combat terrorism in the region and the world."

It is believed that much of the intelligence collected under the Five Eyes arrangement can be accessed by any of the Five Eyes partners at any time. Shared NSA-GCHQ wikis are used by both parties to exchange surveillance tips[53] and leaked NSA documents reveal that different Five Eyes partners have created shared and integrated databases, as revealed by one NSA document that references "GCHQ-accessible 5-eyes [redacted] databases."[54] One Guardian article explained:

> "Gaining access to the huge classified data banks appears to be relatively easy. Legal training sessions – which may also be required for access to information from Australian, Canadian, or New Zealand agencies – suggest that gaining credentials for data is relatively easy. The sessions are often done as self-learning and self-assessment, with "multiple choice, open-book" tests done at the agent's own desk on its "iLearn" system. Agents then copy and paste their passing result in order to gain access to the huge databases of communications."[55]

A core programme that provides this capability is known as XKEYSCORE. That has been described by internal NSA presentations as an "analytic framework" which enables a

---

[51] The Puzzle Palace: A Report on America's Most Secret Agency, James Bamford, accessible at: http://cryptome.org/jya/pp08.htm

[52] http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10695100

[53] http://mobile.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=2,all&hp=&_r=0; the New Zealand GCSB's 2001/2012 Annual Report refers the GCSB being able "to leverage off the training programmes of its overseas partners to increase opportunities for staff to develop their tradecraft skills. Available at: http://www.gcsb.govt.nz/newsroom/annual-reports/Annual%20Report%202012.pdf, p. 11.

[54] US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, 20 August 2013, available at: http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data#

[55] Portrait of the NSA: no detail too small in quest for total surveillance, 2 November 2013, accessible at: http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance

single search to query a "3-day rolling buffer" of "all unfiltered data" stored at 150 global sites on 700 database servers.[56]

The NSA XKEYSCORE system has sites that appear in Five Eyes countries,[57] with the New Zealand's Waihopai Station, Australia's Pine Gap, Shoal Bay, Riverina and Geraldton Stations, and the UK's Menwith Hill base all present. It has been confirmed that all these bases use XKEYSCORE and "contribute to the program."[58] The system indexes e-mail addresses, file names, IP addresses and port numbers, cookies, webmail and chat usernames and buddylists, phone numbers, and metadata from web browsing sessions including searches queried among many other types of data that flows through their collection points. It has been reported that XKEYSCORE

> "processes all signals before they are shunted off to various "production lines" that deal with specific issues and the exploitation of different data types for analysis - variously code-named NUCLEON (voice), PINWALE (video), MAINWAY (call records) and MARINA (internet records)"[59]

One of these programmes, MARINA, "has the ability to look back on the last 365 days' worth of DNI metadata seen by the SIGINT collection system, regardless whether or not it was tasked for collection"[60] giving Five Eyes partners the ability to look back on a full year's history for any individual whose data was collected – either deliberately or incidentally – by the system.

The no-spy deal myth

While UKUSA is often reported as having created a 'no spy pact' between Five Eyes States, there is little in the original text to support such a notion. Crucially, first and foremost no clause exists that attempts in any form to create such an obligation. Instead, if anything the converse is true: the scope of the arrangement consciously carves out space to permit State-on-State spying even by parties to UKUSA. It limits the scope to governing the "relations of above-mentioned parties in communications intelligence matters only" and more specifically that the "exchange of such … material … is not prejudicial to national interests."[61]

Additionally, while the text mandates that each party shall "maintain, in the country of the other, a senior liaison officer accredited to the other," once again the text is caveated, stating that

[56] http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation
[57] http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation page 5
[58] http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html
[59] http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html
[60] http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents
[61] page 9

> "[l]iaison officers of one party shall normally have unrestricted access to those parts of the other's agencies which are engaged directly in the production of COMINT, except such parts thereof which contain unexchangable information."[62]

As best can be ascertained, therefore, it seems there is no prohibition on intelligence-gathering by Five Eyes States with respect to the citizens or residents of other Five Eyes States. There is instead, it seems, a general understanding that citizens will not be directly targeted, and where communications are incidentally intercepted there will be an effort to minimize the use and analysis thereof by the intercepting State. This analysis has been confirmed by a leaked draft 2005 NSA directive entitled "Collection, Processing and Dissemination of Allied Communications."[63] This directive carries the classification marking "NF" meaning "No Foreign", short for "NOFORN" or "Not Releasable to Foreign Nationals." The directive states:

> "Under the British-U.S. Communications Intelligence Agreement of 5 March 1946 (commonly known as the United Kingdom/United States of American (UKUSA) Agreement), both governments agreed to exchange communications intelligence products, methods and techniques as applicable so long as it was not prejudicial to national interests. This agreement has evolved to include a common understanding that both governments will not target each other's citizens/persons. However when it is in the best interest of each nation, each reserve the right to conduct unilateral COMINT against each other's citizens/persons. Therefore, under certain circumstances, it may be advisable and allowable to target Second Party persons and second party communications systems unilaterally when it in the best interests of the U.S and necessary for U.S national security. Such targeting must be performed exclusively within the direction, procedures and decision processes outlined in this directive."[64]

The directive continues:

> "When sharing the planned targeting information with a second party would be contrary to US interests, or when the second party declines a collaboration proposal, the proposed targeting must be presented to the signals intelligence director for approval with justification for the criticality of the proposed collection. If approved, any collection, processing and dissemination of the second party information must be maintained in NoForn channels."[65]

Significantly, the details of some NSA programmes, not intended to be shared with Five Eyes countries, indicate that intelligence collection is taking place in Five Eyes partner countries. NSA's big data analysis and data visualization system BOUNDLESS

---

[62] page 23
[63] US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, 20 August 2013, available at: http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data#
[64] Draft 2005 directive, reprinted in "US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data," *The Guardian,* 20 August 2013, available at: http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data#
[65] Ibid.

INFORMANT[66] are marked "TOP SECRET//SI//NOFORN". These documents show that in March 2013 the agency collected 97 billion pieces of intelligence from computer networks worldwide. The document grades countries based on a color scheme of green (least subjected to surveillance) through to yellow and orange and finally, red (most surveillance). Five Eyes partners are not excluded from the map and instead are shaded green, which is suggestive that some collection of these States' citizens or communications is occurring.

Changes to the original arrangement, however, suggest a convention is in place between at least two of the Five Eyes partners – UK and US – that prevents deliberate collection or targeting of each other's citizens unless authorised by the other State. The 2005 draft directive states: "[t]his agreement [UKUSA] has evolved to include a common understanding that both governments will not target each other's citizens/persons." This of course has not prevented spying without consent, but it appears it is preferable that when Five Eyes partners want to spy on another member of the agreement, they do so with the other country's consent. It is unclear on what basis consent may be given or withheld, but the directive explains:

> "There are circumstances when targeting of second party persons and communications systems, with the full knowledge and co-operation of one or more second parties, is allowed when it is in the best interests of both nations."[67]

The directive goes on to state that these circumstances might include "targeting a UK citizen located in London using a British telephone system;" "targeting a UK person located in London using an internet service provider (ISP) in France;" or "targeting a Pakistani person located in the UK using a UK ISP."

Historically, the Five Eyes members expected each other to make attempts to minimise the retention and dissemination of information about Five Eyes partners once intercepted. Duncan Campbell explains:

> "New Zealand officials were instructed to remove the names of identifiable UKUSA citizens or companies from their reports, inserting instead words such as "a Canadian citizen" or "a US company". British COMINT staff have described following similar procedures in respect of US citizens following the introduction of legislation to limit NSA's domestic intelligence activities in 1978. The Australian government says that "DSD and its counterparts operate internal procedures to satisfy themselves that their national interests and policies are respected by the others … the Rules [on SIGINT and Australian persons] prohibit the dissemination of information relating to Australian persons gained accidentally during the course of routine collection of foreign communications; or the reporting or recording of the

[66] David Cameron's phone 'not monitored' by US, BBC News, 26th October 2013, available at: http://www.theguardian.com/world/interactive/2013/jun/08/nsa-boundless-informant-data-mining-slides
[67] US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, 20 August 2013, available at: http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data#

names of Australian persons mentioned in foreign communications."[68]

A 2007 document explains that this is no longer an expectation, as the Five Eyes are consenting to the broad trawling of data incidentally intercepted by other Five Eyes partners. The document explains:

> "Sigint [signals intelligence] policy … and the UK Liaison Office here at NSAW [NSA Washington] worked together to come up with a new policy that expands the use of incidentally collected unminimized UK data in SIGINT analysis[…] Now SID analysts can unminimize all incidentally collected UK contact identifiers, including IP and email addresses, fax and cell phone numbers, for use in analysis."[69]

Outside the Second Party partners that make up the Five Eyes, there is no ambiguity about who else can be spied on, including third party partners. An internal NSA presentation made clear "[w]e can, and often do, target the signals of most 3rd party foreign partners."[70] In other words, the intelligence services of the Five Eyes agencies may spy on each other, with some expectation that they will be consulted when this occurs; everyone else is fair game, even if they have a separate intelligence-sharing agreement with one or several Five Eyes members.

This understanding that allies may still be spied upon has been echoed in other public statements made by the US, which in the wake of the Snowden revelations has confirmed, through an unnamed senior official, that "we have not made across the board changes in policy like, for example, terminating intelligence collection that might be aimed at all allies."[71]

Spying on heads of State

Questions remain, however, as to whether arrangements within Five Eyes may prevent the surveillance of the respective heads of States of Five Eyes partners. It has been confirmed by the White House that UK Prime Minister David Cameron's communications "have not, are not and will not be monitored by the US."[72] However, while New Zealand Prime Minister John Key has agreed that he is satisfied that the US has not spied on him and that he is "confident of the position," he will not confirm whether this is because the Five Eyes members have agreed to this.[73] Additionally after German Chancellor Angela

---

[68] http://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf page 3
[69] http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data#
[70] http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html
[71] Feinstein: White House Will Stop Spying on Allies. White House: Not So Fast , The Atlantic Wire, 28th October 2013, available at: http://www.thewire.com/politics/2013/10/sen-feinstein-white-house-will-stop-spying-allies/71023/
[72] http://www.bbc.co.uk/news/uk-politics-24668861
[73]John Key, 29 October 2013, Post-Cabinet Press Conference, audio available at: http://www.scoop.co.nz/stories/HL1310/S00224/pms-press-conference-audio-meridian-spying-and-fonterra.htm
Key confident US didn't spy on him, Stuff.co.nz, 29th October 2013, available at: http://www.stuff.co.nz/national/politics/9338530/Key-confident-US-didn-t-spy-on-him

Merkel demanded[74] that the United States sign a no-spy agreement to prohibit the bilateral spying between nations, the US has indicated that while they would be willing to engage in "a new form of collaboration" a no-spy pact is not on the table.[75]

Allied spying more broadly is a common activity. In 1960, when Bernon Mitchell and William Martin infamously defected to the Soviet Union, they revealed the scope of NSA's activities, reporting that:

> "We know from working at NSA [that] the United States reads the secret communications of more than forty nations, including its own allies… NSA keeps in operation more than 2000 manual intercept positions… Both enciphered and plain text communications are monitored from almost every nation in the world, including the nations on whose soil the intercept bases are located."[76]

Other surveillance partnerships

Over almost seven decades, the Five Eyes alliance has splintered notably only once when, in 1985, New Zealand's new Labour Government refused to allow a US ship to visit New Zealand, in accordance with the government's anti-nuclear policy (not to allow ships into its New Zealand waters without confirmation they were neither nuclear-powered, nor carrying nuclear weapons). This policy was turned into law in 1987 with the creation of the New Zealand Nuclear Free Zone.[77] The political fallout from the introduction of the policy included the splintering off of New Zealand, at least temporarily, from the Five Eyes, and the creation of a Four Eyes alliance with the acronym ACGU. This split has been confirmed in a number of military classification marking documents.[78] It is understood that there was some distancing of New Zealand from the Five Eyes in the years immediately following the incident, but that the schism was less significant than previously thought;[79] by making reference to documents dated in the past decade, released as part of the Snowden leaks, it is clear that New Zealand remains an integral part of the Five Eyes alliance.

---

[74] Germany to seek 'no spying' deal with US, Financial Times, 12th August 2013, available at: http://www.ft.com/cms/s/0/67eef7f4-0375-11e3-980a-00144feab7de.html

[75] Germans Rejected: US Unlikely to Offer 'No-Spy' Agreement, Der Spiegel, 12th November 2013, available at: http://www.spiegel.de/international/germany/us-declines-no-spy-pact-with-germany-but-might-reveal-snowden-secrets-a-933006.html

[76] Inside Echelon, Duncan Campbell, 2000, available at: http://www.heise.de/tp/artikel/6/6929/1.html

[77] New Zealand Nuclear Free Zone, Disarmament, and Arms Control Act 1987: s 9(2) states "The Prime Minister may only grant approval for the entry into the internal waters of New Zealand by foreign warships if the Prime Minister is satisfied that the warships will not be carrying any nuclear explosive device upon their entry into the internal waters of New Zealand." Section 11 states "Entry into the internal waters of New Zealand by any ship whose propulsion is wholly or partly dependent on nuclear power is prohibited.")

[78] http://www.afcea.org/events/pastevents/documents/LWN11_Track_1_Session_5.pdf; https://www2.centcom.mil/sites/foia/rr/CENTCOM%20Regulation%20CCR%2025210/Wardak%20CH-47%20Investigation/r_EX%2060.pdf

[79] See, Nicky Hager, Secret Power, 1996, pp. 23-24.

Additionally, other 'Eyes-like' relationships exist, in various forms with membership ranging through 3-, 4-, 6-, 7-, 8-, 9- and 10- and 14-Eyes communities. These 'Eyes' reference different communities with varying focuses dealing with military coalitions, intelligence partnerships with many having established dedicated communication networks.[80] The Guardian describes two such arrangements:

> "the NSA has other coalitions, although intelligence-sharing is more restricted for the additional partners: the 9-Eyes, which adds Denmark, France, the Netherlands and Norway; the 14-Eyes, including Germany, Belgium, Italy, Spain and Sweden; and 41-Eyes, adding in others in the allied coalition in Afghanistan."[81]

This is supported by statements made by an ex-senior NATO intelligence officer:

> "The Five Eyes SIGINT community also plays a 'core' role in a larger galaxy of SIGINT organizations found in established democratic states, both west and east. Five Eyes 'plus' gatherings in the west include Canada's NATO allies and important non-NATO partners such as Sweden. To the east, a Pacific version of the Five Eyes 'plus' grouping includes, among others, Singapore and South Korea. Such extensions add 'reach' and 'layering' to Five Eyes SIGINT capabilities."[82]

A New York Times article[83] again confirms such groups exist by acknowledging "[m]ore limited cooperation occurs with many more countries, including formal arrangements called Nine Eyes and 14 Eyes and Nacsi, an alliance of the agencies of 26 NATO countries." Different intelligence co-operation groups also exist outside the broader abovementioned structures dealing with narrower areas of collaboration.[84] Within these groups, no attempt to create a no-spy deal has been made; these countries "can gather intelligence against the United States through CNE (computer network exploitation) and therefore share CNE and CND (Computer Network Defense) can sometimes pose clear risks."[85]

---

[80] http://electrospaces.blogspot.co.uk/2013/11/five-eyes-9-eyes-and-many-more.html
[81] http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance
[82] Canada and the Five Eyes Intelligence Community, James Cox, Strategic Studies Working Group Papers, December 2012, accessible at: http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf page 7
[83] No Morsel Too Minuscule for All-Consuming N.S.A. , New York Times, 2nd November, 2013 http://mobile.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=2,all&hp=&_r=0
[84] One co-operation group is mentioned in an NSA document entitled "sharing computer networking operations cryptologic information with foreign partners". This document names the Five Eyes partnership a "Tier A" group that has 'comprehensive cooperation.' The much larger "Tier B" of 19 countries has 'focused co-operation' and is mostly made up of European States, except Japan, Turkey and South Korea. The full list includes Austria, Belgium, Czech Republic, Denmark, Germany, Greece, Hungry, Iceland, Italy, Japan, Luxembourg, Netherlands, Norway, Poland, Portugal, South Korea, Spain, Sweden, Switzerland and Turkey.
El CNI facilitó el espionaje masivo de EEUU a España , El Mundo, 10th October, 2013, accessible at: http://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html
[85] El CNI facilitó el espionaje masivo de EEUU a España , El Mundo, 10th October, 2013, accessible at: http://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html

It was reported[86] in 2010 when the UKUSA documents were first released, that "Norway joined [the eavesdropping network] in 1952, Denmark in 1954, and Germany in 1955" and that "Italy, Turkey, the Philippines and Ireland are also members." This however has been contested with a journalist working on the current Snowden documents staying they were "confused by that reference."[87]

The NATO Special Committee, made up of the heads of the security services of NATO member countries, also provides a platform for intelligence sharing, although due to the alliances diverse and growing membership it is thought there are concerns about sharing sensitive military and SIGINT documents on a systematic basis.[88] As explained by Scheinen and Vermeulen,[89] however:

> "The Agreement between the parties to the North Atlantic Treaty for the security of information of 1949 is quite short, but article 5 for instance gives states carte blanche 'to make any other agreement relating to the exchange of classified information originated by them,' leaving room for many technically detailed arrangements in which the actual cooperation is being regulated."

[86] http://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released
[87] https://twitter.com/jamesrbuk/status/403643887685611520
[88] The 28 NATO countries are Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, United States,
[89] Scheinin, M and Vermeulen, M, "Intelligence cooperation in the fight against terrorism through the lens of human rights law and the law of state responsibility," in Born, Leigh and Wills (eds), *International Intelligence Cooperation and Accountability* (Oxon: Routledge, 2011), 256.

Chapter Two – Secret law is not law

The intelligence agencies of the Five Eyes countries conduct some of the most important, complex and far-reaching activities of any State agency, and they do so under behind the justification of a thicket of convoluted and obfuscated legal and regulatory frameworks. The laws and agreements that make up the Five Eyes arrangement and apply it to domestic contexts lack any semblance of clarity or accessibility necessary to ensure that the individuals whose rights and interests are affected by them are able to understand their application. As such, they run contrary to the fundamental building blocks of the rule of law.

The rule of law and accessibility

The accessibility of law is a foundational element the rule of law. Many have different views of what exactly constitutes the rule of law, but it is widely understood to play a critical role in checking excessive or arbitrary power. Core to the rule of law is the idea that all individuals are able to know what law is exercised over them by those in power, and how conduct must be accordingly regulated to ensure it is in compliance with such laws. Lord Neuberger's first principle of the rule of law explains just how critical the accessibility of law is to the rule of law:

> "At its most basic, the expression connotes a system under which the relationship between the government and citizens, and between citizen and citizen, is governed by laws which are followed and applied. That is rule by law, but the rule of law requires more than that. First, the laws must be freely accessible: that means as available and as understandable as possible."[90]

If law itself isn't published in a clear and understandable way then citizens cannot evaluate when an action by another person, or by their government, is unlawful. As Tom Bingham explains, "if the law is not sufficiently clear, then it becomes inaccessible; if people cannot properly access (i.e. understand) the law that they are governed by, then so far as they are concerned, they are being governed by arbitrary power." For all actions by the State there must be a legal justification. Simply because there is law on the statute books does not necessarily mean that it isn't arbitrary.

Accessing the laws regulating the actions of the Five Eyes

It has been alleged that "there is no formal over-arching international agreement that governs all Five Eyes intelligence relationships,"[91] but rather a myriad of memoranda,

[90] http://www.supremecourt.gov.uk/docs/speech-131015.pdf
[91] Canada and the Five Eyes Intelligence Community, James Cox, Strategic Studies Working Group Papers, December 2012, accessible at: http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf

agreements, and conventions that must be considered in tandem with complex national legislation.

Scheinin and Vermeulen argue that

> "The overwhelming majority of these intelligence cooperation arrangements are secret – or at least they are never published nor registered at the UN Secretariat pursuant to Article 102 of the UN Charter.[92] From the perspective of international law they are likely to fall within a murky area of 'non-treaty arrangements', which can include arrangements such as 'memoranda of understanding', 'political agreements' 'provisional understanding', 'exchanges of notes', 'administrative agreements', 'terms of reference', 'declarations' and virtually every other name one can think of."[93]

However, taken together, the Five Eyes agreements arguably rise to the level of an enforceable treaty under international law. It is clear from their scope and wide-reaching ramifications that the Five Eyes agreements implicate the rights and interests of individuals sufficiently to raise the agreements to the level of legally-binding treaty.

In any event, it is impossible to know whether the initial intentions of the drafters or the scope of the legal obligations created under the agreements elevate them to the status of legally-binding treaty because the agreements are completely hidden from public view. Indeed, not only are the public unable to access and scrutinise the agreements that regulate the actions of the Five Eyes, but even the intelligence services themselves do not have a complete picture of the extent of intelligence sharing activities. The NSA admitted during legal proceedings in 2011 that the information-gathering infrastructure was so complex that "there was no single person with a complete understanding." [94]

The domestic legal frameworks implementing the obligations created by the Five Eyes obligations are equally obfuscated. With respect to the US, for example, the NSA acknowledged in a recently-released strategy document that

> "[t]he interpretation and guidelines for applying [American] authorities, and in some cases the authorities themselves, have not kept pace with the complexity of the technology and target environments, or the operational expectations levied on NSA's mission."[95]

---

page 4

[92] Article 102 of the UN Charter states that: 1. Every treaty and every international agreement entered into by any Member of the United Nations after the present Charter comes into force shall as soon as possible be registered with the Secretariat and published by it. 2. No party to any such treaty or international agreement which has not been registered in accordance with the provisions of paragraph 1 of this Article may invoke that treaty or agreement before any organ of the United Nations.

[93] Scheinin, M and Vermuelen, M, "Intelligence cooperation in the fight against terrorism through the lens of human rights law and the law of state responsibility," in Born, Leigh and Wills (eds), *International Intelligence Cooperation and Accountability* (Oxon: Routledge, 2011), 256.

[94]http://www.theregister.co.uk/Print/2013/09/11/declassified_documents_show_nsa_staff_abused_tapping_misled_courts/

[95] (U) SIGINT Strategy, 2012-2016, 23 February 2012

The chair of the Senate intelligence committee, Diane Feinstein, has strongly criticised the actions taken by the NSA under the purported ambit of the relevant legislation, noting that "[…] it is clear to me that certain surveillance activities have been in effect for more than a decade and that the Senate Intelligence Committee was not satisfactorily informed."[96]

In the UK, the Intelligence and Security Committee – in charge of overseeing the actions of the UK intelligence agencies, including GCHQ – have responded to the Snowden leaks by remarking:

> "It has been alleged that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications […] and we are satisfied that they conformed with GCHQ's statutory duties. The legal authority for this is contained in the Intelligence Services Act 1994."[97]

Yet the chair of the ISC has in fact admitted to confusion about whether "if British intelligence agencies want to seek to know the content of emails can they get round the normal law in the UK by simply asking an American agencies to provide that information?"[98]

When the head of the committee charged with overseeing the lawfulness of the actions of intelligence services is unsure as to whether such agencies have acted lawfully, there is plainly a serious dearth in the accessibility of law, calling into question the rule of law. Without law that is accessible, citizens are unable to regulate their conduct or scrutinise that of their governments. In such circumstances, it is impossible to verify whether governments are acting in accordance with the law as required of them under human rights law.

Ensuring the Five Eyes act 'in accordance with the law'

There is a significant body of European Court of Human Rights jurisprudence on what constitutes interference "in accordance with the law" in the context of secret surveillance and information gathering, such as that undertaken by the Five Eyes.

The Court begins from the perspective that surveillance, particularly secret surveillance, is a significant infringement on human rights, and in order to be justified under the European Convention on Human Rights must be sufficiently clear and precise "to give citizens an adequate indication as to the circumstances in which and the conditions on

---

[96] Paul Lewis and Spencer Ackerman, "NSA: Dianne Feinstein breaks ranks to oppose US spying on allies," *The Guardian,* 29 October 2013, available at http://www.theguardian.com/world/2013/oct/28/nsa-surveillance-dianne-feinstein-opposed-allies.

[97] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf

[98] Nicholas Watts, "GCHQ 'broke law if it asked for NSA intelligence on UK citizens', The Guardian, 10 June 2013, available at http://www.theguardian.com/world/2013/jun/10/gchq-broke-law-nsa-intelliegence

which public authorities are empowered to resort to this secret and potentially dangerous interference."[99]

It must be clear "what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive" and the law must indicate "with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities"[100] in order that individuals may have some certainty about the laws to which they are subject and regulate their conduct accordingly.

Yet "the degree of certainty will depend on the circumstances."[101] As the Court has noted, "foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly..."[102]

Where a power vested in the executive is exercised in secret, however, the risks of arbitrariness are evident: in the words of the Court in *Weber v Germany,* "a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it."[103] In such circumstances, "is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated…"[104]

What, then, does human rights law require of a law in order to ensure secret surveillance does not infringe the principles of accessibility and foreseeability? The Court's decision in *Weber* is authoritative on this point:

> "In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."[105]

[99] Malone v United Kingdom (1985) 7 EHRR 14 [67]
[100] Ibid, at [79].
[101] Ormerod., R. and Hooper, Blackstone's Criminal Practice 2012, London 2012.
[102] *Weber v Germany,* Application 54934/00, (2008) 46 EHRR SE5 at [77.]
[103] Ibid, at [106].
[104] Kruslin v France (1990) 12 EHHR 547, at [33].
[105] Ibid, at [95]

Applying human rights requirements to the laws of the Five Eyes

There is no clear and accessible legal regime that indicates the circumstances in which, and the conditions on which, Five Eyes authorities can request access to signals intelligence from, or provide such intelligence, to another Five Eyes authority. Each of the Five Eyes states have broad, vague domestic laws that purport to warrant the sharing of and access to shared signal intelligence with the authorities of other States, but fail to set out minimum safeguards or provide details of or restrictions upon the nature of intelligence sharing.

In the **United Kingdom**, the ISC has indicated that the authority to share and receive intelligence is granted by the *Intelligence Services Act 1994*. Section 3(1) of the 1994 Act specifies the functions of GCHQ in these terms:

> (1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be –
>
> (a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and
>
> (b) to provide advice and assistance [...]"

Section 3(2) of the 1994 Act specifies the purposes for which the functions referred to in s3(1)(a) shall be exercisable, and makes clear that they shall be exercisable only -

> (a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
> (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or
> (c) in support of the prevention or detection of serious crime.

Section 4(2)(a) of the 1994 Act imposes on the Director of GCHQ a duty to ensure –

> (a) that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings.

In the **United States**, the scope of intelligence activities was initially set down in Executive Order 12333 – United States intelligence activities, of December 4, 1981.[106] Even though the structure of the United States intelligence community changed considerably after 9/11, the powers granted in the Executive Order nevertheless continue to be invoked.

[106] http://www.archives.gov/federal-register/codification/executive-order/12333.html#1.9

Section 1.12 (b) provides that the responsibilities of the National Security Agency shall include, inter alia:

> (5) Dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the Government, including the military services, in accordance with guidance from the Director of Central Intelligence;
> (6) Collection, processing and dissemination of signals intelligence information for counterintelligence purposes;
> (7) Provision of signals intelligence support for the conduct of military operations in accordance with tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provision of such support requires use of national collection systems, these systems will be tasked within existing guidance from the Director of Central Intelligence;
> […]
> (12) Conduct of foreign cryptologic liaison relationships, with liaison for intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence […]

Section 1.7 deals with the responsibilities of Senior Officials of the Intelligence Community, and designates the following responsibility to the Director of Central Intelligence:

> (f) Disseminate intelligence to cooperating foreign governments under arrangements established or agreed to by the Director of Central Intelligence […]

Section 1.8 relates to the Central Intelligence Agency, and includes among that body's functions to

> (a) Collect, produce and disseminate foreign intelligence and counterintelligence, including information not otherwise obtainable […]

The legislation in **Australia** is slightly more detailed with regards to the circumstances in which intelligence can be shared with and received from foreign intelligence agencies. The actions of the Australian intelligence agencies are governed by the *Intelligence Services Act 2001*, section 7 of which articulates the functions of the Australian Signals Directorate, which include

> (1) to obtain intelligence about the capabilities, intentions or activities of people or organisations outside Australia in the form of electromagnetic energy, whether guided or unguided or both, or in the form of electrical, magnetic or acoustic energy, for the purposes of meeting the requirements of the Government, and in particular the requirements of the Defence Force, for such intelligence; and
> (2) to communicate, in accordance with the Government's requirements, such intelligence; and
> (3) to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; […]

Pursuant to s11(2AA) of the Act, intelligence agencies may communicate incidentally obtained intelligence to appropriate Commonwealth or State authorities or to authorities of other countries approved under paragraph 13(1)(c) if the intelligence relates to the involvement, or likely involvement, by a person in one or more of the following activities:

(a) activities that present a significant risk to a person's safety;
(b) acting for, or on behalf of, a foreign power;
(c) activities that are a threat to security;
(d) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
(e) committing a serious crime.

Section 13(1)(c) permits the agency to cooperate with "authorities of other countries approved by the Minister as being capable of assisting the agency in the performance of its functions."

The **New Zealand** similarly provides the Government Communications Security Bureau with broad powers and functions, including under section 8A

(a) to co-operate with, and provide advice and assistance to, any public authority whether in New Zealand or overseas, or to any other entity authorised by the Minister, on any matters relating to the protection, security, and integrity of—
    (i) communications, including those that are processed, stored, or communicated in or through information infrastructures; and
    (ii)information infrastructures of importance to the Government of New Zealand; […]

and under section 8B

(a) to gather and analyse intelligence (including from information infrastructures) in accordance with the Government's requirements about the capabilities, intentions, and activities of foreign persons and foreign organisations; and
(b) to gather and analyse intelligence about information infrastructures; and
(c) to provide any intelligence gathered and any analysis of the intelligence to—
    (i) the Minister; and
    (ii) any person or office holder (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence.

Section 8B(2) also sanctions the sharing of information with foreign intelligence authorities, stipulating "[f]or the purpose of performing its function under subsection (1)(a) and (b), the Bureau may co-operate with, and provide advice and assistance to, any public authority (whether in New Zealand or overseas) and any other entity authorised by the Minister for the purposes of this subsection."

In **Canada,** the functions of the Communications Security Establishment Canada (CSEC) are articulated in Part V.1 to the *National Defence Act*. Section 273.64(1) sets out CSEC's three-part mandate, namely

(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

Part V.1 of the *National Defence Act* in relation to CSEC does not contain any provisions on cooperation with other agencies, including foreign agencies.

An analysis of these cursory legal provisions reveals that they fall far short of describing the fluid and integrated intelligence sharing activities that take place under the ambit of the Five Eyes arrangement with sufficient clarity and detail to ensure that individuals can forsee their application. None of the domestic legal regimes set out the circumstances in which intelligence authorities can obtain, store and transfer nationals' or residents' private communication and other information that are intercepted by another Five Eyes agency, nor which will govern the circumstances in which any of the Five Eyes States can request the interception of communications by another party to the alliance. The same applies to obtaining private information such as emails, web-histories etc. held by internet and other telecommunication companies. There is there a legal regime that indicates, once such communications are provided to the authorities of one State, the procedure for examining, using or storing the communication, the conditions for transferring it to third parties and the circumstances in which it will be destroyed.

The legal and regulatory frameworks that govern and give effect to Five Eyes cannot be said to be sufficiently clear and detailed to meet the requirement of being "in accordance with the law," nor they are they sufficiently accessible to ensure that they comply with the rule of law. Secret, convoluted or obfuscated law can never be considered law within a democratic society governed by the rule of law. The actions of the Five Eyes run completely contrary to the fundamental building blocks of such a society.

Chapter Three – Holding the Five Eyes to account

The recent revelations of global surveillance practices have prompted a fundamental re-examination of the responsibility of States under international law with respect to cross-border surveillance. The patchwork of secret spying programmes and intelligence-sharing agreements implemented by parties to the Five Eyes arrangement constitutes an integrated global surveillance arrangement that now covers the majority of the world's communications.

At the heart of this arrangement are carefully constructed legal frameworks that provide differing levels of protections for internal versus external communications, or those relating to nationals versus non-nationals. These frameworks attempt to circumvent national constitutional or human rights protections governing interferences with the right to privacy of communications that, States contend, apply only to nationals or those within their territorial jurisdiction.

In doing so, the Five Eyes states not only defeat the spirit and purpose of international human rights instruments; they are in direct violation of their obligations under such instruments. Human rights obligations apply to all individuals subject to a State's jurisdiction.[107] Jurisdiction extends not only to the territory of the State, but to anyone within the power and effective control of the State, even if they are outside the territory.[108] It is argued here that jurisdiction extends to situations where a State interferes with the right to privacy of an individual whose communications are intercepted, stored or processed within that State's territory. In such circumstances, the State owes obligations to that individual regardless of their location.

By understanding State jurisdiction over human rights violations in this way we can give effect to international human rights obligations in the digital age. Through the concept of "interference-based jurisdiction", whereby, subject to permissible limitations, States owe a general duty not to interfere with communications that pass through their territorial borders, mass surveillance is cognisable within a human rights framework in a way that provides rights and remedies to affected individuals. Without such a perspective on responsibility for violations that properly reflects the nature and scope of Five Eyes surveillance, and the way in which privacy violations occur, States will continue to conduct surveillance in a way that renders human rights obligations meaningless.

---

[107] ICCPR, Article 2: "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction…"; ECHR, Article 1: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention;" American Convention on Human Rights, Article 1: "The States Parties to this Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms, without any discrimination for reasons of race, color, sex, language, religion, political or other opinion, national or social origin, economic status, birth, or any other social condition."

[108] Human Rights Committee General Comment 31, para 10.

We seek to introduce an alternative perspective on jurisdiction and to further understandings of how human rights law can be understood in the digital age. Our intention is to supplement - not to detract from – other arguments around how jurisdiction in international human rights law functions in relation to mass surveillance. For example, interferences occurring outside the territory of the state may be attributable to that state under the ordinary principles of state responsibility. However, we are concerned exclusively with a State's obligations in relation to interferences with the right to privacy (when communications are collected, stored or processed) occurring within the physical territory of that State.

The right to privacy of communications

The right to privacy is an internationally recognized right. Article 17 (1) of the International Covenant on Civil and Political Rights provides

> "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."

According to the United Nations Human Rights Committee, in its General Comment No. 16:

> "Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[109]

Article 8 of the European Convention on Human Rights provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society".

The European Court of Human Rights has consistently held that the interception of telephone communications, as well as facsimile and e-mail communications content,[110] are covered by notions of "private life" and "correspondence" and thus constitute an interference with Article 8.[111]

Importantly the European Court has found[112] the interception and/or storage of a communication constitutes the violation, and that the "subsequent use of the stored

[109] CCPR General Comment No. 16: Article 17 (Right to Privacy), para. 8.
[110] Liberty & Ors v United Kingdom (2008) Application 58243/00
[111] See Malone v United Kingdom (1985) 7 EHRR 14 [64]; Weber v Germany (2008) 46 EHRR SE5 at [77]; and Kennedy v United Kingdom (2011) 52 EHRR 4 at [118]).
[112] Amann v Switzerland (2000) application 27798/95; Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48

information has no bearing on that finding"[113] nor does it matter "whether the information gathered on the applicant was sensitive or not or as to whether the applicant had been inconvenienced in any way."[114] It is argued that the same reasoning applies to the processing of communications.

Therefore, the right to privacy, extending as it does to the privacy of communications, is a relatively unusual right in the sense that its realization can occur remotely from the physical location of the individual.

When an individual sends a letter, email or a text-message, or makes a phone call, that communication leaves their physical proximity and travels to its destination. In the course of its transmission the communication may pass through multiple other States and, therefore, multiple jurisdictions. The right to privacy of the communication remains intact, subject only to the permissible limitations set out under human rights law.[115]

Mass surveillance as a breach of the right to privacy of communications

The Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion has described the invasiveness of mass interception of fibre optic cables:[116]

> "By placing taps on the fibre optic cables, through which the majority of digital communication information flows, and applying word, voice and speech recognition, States can achieve almost complete control of tele- and online communications."

The Special Rapporteur reasons that "[m]ass interception technology eradicates any considerations of proportionality, enabling indiscriminate surveillance. It enables the State to copy and monitor every single act of communication in a particular country or area, without gaining authorization for each individual case of interception."[117]

Mass surveillance has also been found to be an interference with the right to privacy under European human rights law. In *Weber and Saravia v Germany* (2006) Application 54934/00, the Court reiterated that

> "the mere existence of legislation which allows a system for the

[113] Amann v Switzerland (2000) application 27798/95 para 69
[114] Amann v Switzerland (2000) application 27798/95 para 70
[115] A comprehensive account of the permissible limitations on the right to privacy is presented in the report of the UN Special Rapporteur on the freedom of expression and opinion of 17 April 2013 (A/HRC/23/40).
[116] Report of the Special Rapporteur on promotion and protection of the right to freedom of expression and opinion, Frank La Rue, 17 April 2013, A/HRC/23/40, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, at para. 38.
[117] Ibid, para. 62.

> secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them."

The collection and storage of data that relates to an individual's private life is so invasive, and brings with it such risk of abuse, that it alone amounts to an interference with the right to privacy, according to European Court of Human Rights jurisprudence.[118] Accordingly, mass surveillance programmes must violate international law.

Jurisdiction and human rights obligations

Traditional conceptions of State human rights obligations focus on a nexus between the territory where the obligation is owed and an individual's connection with that territory (by virtue of nationality, residence or physical location within it). In the context of obligations under international human rights treaties, jurisdiction has traditionally served as a doctrinal bar to the recognition and realization of human rights obligations extra-territorially. Although, as noted by Milanovic:

> "[q]uestions as to when a state owes obligations under a human rights treaty towards an individual located outside its territory are being brought more and more frequently, before courts both international and domestic. Victims of aerial bombardment[119], inhabitants of territories under military occupation[120] – including deposed dictators[121], suspected terrorists detained in Guantanamo by the United States[122], and the family of a former KGB spy who was assassinated in London through the use of a radioactive toxin, allegedly at the orders or with the collusion of the Russian government[123] – all of these people have claimed protection from human rights law against a state affecting their lives while acting outside its territory."

The jurisdiction clauses in two of the most relevant human rights instruments – the European Convention on Human Rights (ECHR) and the International Covenant on Civil and Political Rights (ICCPR) – are notably different in their construction and numerous

---

[118] S and Marper v United Kingdom (2009) 48 EHRR 50 at [67].
[119] Bankovic and Others v Belgium and Others, App. No. 52207/99, (dec.) [GC], 12 December 2001, hereinafter Bankovic.
[120] *R (Al-Skeini and others) v Secretary of State for Defence*, [2007] UKHL 26, [2007] 3 WLR 33, [2007] 3 All ER 685, on appeal from [2005] EWCA Civ 1609, [2007] QB 140, hereinafter *Al-Skeini*.
[121] *Saddam Hussein v 21 Countries*, App. No. 23276/04, (dec.), March 2006.
[122] See the Conclusions and Recommendations of the Committee against Torture: United States of America, CAT/C/USA/CO/2, 25 July 2006, paras. 14 & 15 and the Concluding Observations of the Human Rights Committee : United States of America, CCPR/C/USA/CO/3, 15 September 2006, para. 10, available at http://www.unhchr.ch/tbs/doc.nsf
[123] See 'Lawyers for slain Russian agent Litvinenko take case to European court', *International Herald Tribune*, 22 November 2007, available at http://www.iht.com/articles/ap/2007/11/23/europe/EU-GEN-Britain-Litvinenko.php?WT.mc_id=rsseurope.

arguments have been mounted to support an understanding of the obligations arising under such treaties as being applicable outside the strict territorial boundaries of the State.

Article 1 of the ECHR holds:

> "The High Contracting Parties shall secure to everyone *within their jurisdiction* the rights and freedoms defined in Section I of this Convention."

In *Al-Skeini v United Kingdom,*[124] the European Court of Human Rights moulded – if not departed from – its earlier jurisprudence in *Banković* [125] to issue a decision that affirms extra-territorial jurisdiction, stating:

> "whenever the State through its agents exercises control and authority over an individual, and thus jurisdiction, the State is under an obligation under Article 1 to secure to that individual the rights and freedoms under Section 1 of the Convention that are relevant to the situation of that individual. In this sense, therefore, the Convention rights can be "divided and tailored" (compare *Banković,* cited above, § 75)."[126]

While Milanovic (2011) notes[127] some inconsistencies in the Court's reasoning, particularly vis a vis *Banković*, crucially the case stands as authority that, although the jurisdictional competence of a State is primarily territorial, it is not limited by territory. It can also extend to those over whom the State exercises authority or control.

In contrast, Article 2(1) of the ICCPR holds:

> "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals *within its territory and subject to its jurisdiction* the rights recognized in the present Covenant…"

In 1966, the International Law Commission, in its Draft Articles on the Law of Treaties (subsequently the Vienna Convention on the Law of Treaties) noted that "[c]ertain types of treaty, by reason of their subject matter, are hardly susceptible of territorial application in the ordinary sense. Most treaties, however, have application to territory and a question may arise as to what is their precise scope territorially."[128]

For the purpose of defining the conditions of applicability of the Covenant, the notion of jurisdiction refers to the relationship between the individual and the state in connection with a violation of human rights, wherever it occurred, so that acts of States that take

---

[124] Application 55721/07, 7 July 2011
[125] Application 52207/99, 12 December 2001
[126] *Bankovic,* at para [73].
[127] http://www.ejiltalk.org/european-court-decides-al-skeini-and-al-jedda/
[128] ILC, 'Draft Articles on the law of Treaties with Commentaries,' (1966) 2 *Yearbook of the International Law Commission* 187 at 213.

place or produce effects outside the national territory may be deemed to fall under the jurisdiction of the state concerned.[129]

As noted above, the right to privacy extends to the privacy of cross-border communications, so that the physical location of the individual may be in a different jurisdiction to that where the interference with the right occurs.

This distinction is examined by Milanovic (2011) who asserts that extraterritorial application can take one of two forms:

> "it will most frequently arise from an *extraterritorial state act,* i.e. conduct attributable to the state, either of commission or of omission, performed outside its sovereign borders… However – and this is a crucial point – extraterritorial application does not *require* an extraterritorial state act, but solely that the individual concerned is located outside the state's territory, while the injury to his rights may as well take place inside it."[130]

With regard to the right to privacy, many violations are not due to extra-territorial acts, but jurisdictional acts with extra-territorial effects. The instances in which jurisdictional acts have extra-territorial effects are infrequent but not without precedent.

One example provided by Milanovic is the question of property rights of foreigners or those absent from the territory. A person may have property rights in the UK by virtue of owning a property in the territory, but may be temporarily or permanently located outside the UK. If the property were to be searched or seized without adherence to legal standards there would be a violation of the individual's right to privacy, regardless of their location at the time of the interference. This is an example of "interference-based" jurisdiction.

A second example is that of enjoyment of Article 6 ECHR fair trial rights during trials in absentia where the individual in question has absconded outside the State's territory. The European Court of Human Rights has repeatedly upheld the right of defendants to enjoy the protections of Article 6 even when they are absent from their trial and outside the territory of the State. In *Sejdovic v Italy,*[131] for example, the Court held, at [91]:

> "Although not absolute, the right of everyone charged with a criminal offence to be effectively defended by a lawyer, assigned officially if need be, is one of the fundamental features of a fair trial (see *Poitrimol*, cited above, § 34). A person charged with a criminal offence does not lose the benefit of this right merely on account of not being present at the trial (see *Mariani v. France*, no. 43640/98, § 40, 31 March 2005)."

---

[129] Delia Salides de Lopez v. Uruguay, Communication No. 52/1979, 13th Sess., at 88, 91 ¶ 12.2, U.N. Doc. CCPR/C/OP/1 (29 July 1981).
[130] Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford: Oxford University Press, 2011).
[131] Application 56581/00, 1 March 2006

A further example is the situation in the European Court of Human Rights' case *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi v Ireland* (2005) 42 EHRR 1, where Irish authorities at Dublin Airport impounded an aircraft that had been leased by a Turkish company from the national airline of the former Yugoslavia. The company argued that the Irish authorities had acted in a way that was incompatible with the European Convention on Human Rights. In considering the issue of jurisdiction, the Court noted the territorial basis of jurisdiction in international law and observed:[132]

> "In the present case it is not disputed that the act about which the applicant company complained, the detention of the aircraft leased by it for a period of time, was implemented by the authorities of the respondent State on its territory following a decision made by the Irish Minister for Transport. In such circumstances the applicant company, as the addressee of the impugned act, fell within the "jurisdiction" of the Irish State, with the consequence that its complaint about that act is compatible ratione loci, personae and materiae with the provisions of the Convention."

With respect to the right to privacy, the European Court has considered at least two cases[133] in which surveillance has involved the interference with the right to privacy of those outside of the respective State's territory. In neither has the Court directly considered the issue of whether obligations owed are extended to individuals outside the territory.

Application to interferences with the right to privacy in the digital age

With the advent of the internet and new digital forms of communication, now most digital communications take the fastest and cheapest route to their destination, rather than the most direct. This infrastructure means that the sender has no ability to choose, nor immediate knowledge of, the route that their communication will take. Even when a digital communication is being sent to a recipient within the same country as the sender, it may travel around the world to reach its destination.

This shift in communications infrastructure means that communications travel through many more countries, are stored in a variety of countries (particularly through the growing popularity of cloud computing) and are thus vulnerable to inception by multiple intelligence agencies. From their bases within the territory of each country, each respective intelligence agency collects and analyses communications that traverse their territory and beyond. While there are many methods used by intelligence agencies to intercept communications, one of the consistent techniques is to exploit the

---

[132] Para 137.

[133] In *Weber and Saravia v. Germany,* Application 54934/00, 29 June 2006, the Court found that the application was inadmissible by other means; in *Liberty and Ors v United Kingdom,* Application 58243/00, 1 July 2008, the Government proceeded on the basis that the applicants could claim to be victims of an interference with their communications sent to or from their offices in the UK and Ireland.

communications infrastructure itself, often in the form of the transnational cables that carry the world's communications.

For more than 50 years the security agencies have intercepted these transnational links. From 1945 onwards the US intelligence agencies systematically intercepted telegraphic data entering or exiting the United States under the codename Project SHAMROCK. As technology developed, newer fibre optic cables were laid that could carry many more communications. These links were also intercepted by intelligence agencies within their territory. Investigative journalist Duncan Campbell explained in 2000 how the NSA was intercepting the foreign communications within US territory:

> "Internet traffic can be accessed either from international communications links entering the United States, or when it reaches major Internet exchanges. Both methods have advantages. Access to communications systems is likely to be remain clandestine - whereas access to Internet exchanges might be more detectable. […] According to a former employee, NSA had by 1995 installed "sniffer" software to collect such traffic at nine major Internet exchange points (IXPs)."[134]

The UK is using more modern versions of this technique to intercept, store and process communications that enter and exit the country in the form of their mass surveillance program TEMPORA. While these undersea fibre-optic cables will land in multiple different countries, due to the UK's geographical position, a disproportionate number of undersea cables land in the UK before they cross the Atlantic Ocean. The Guardian[135] reported that by the summer of 2011, GCHQ had attached probes to more than 200 links within their territory, including at main network switches and undersea cable landing stations. Similar capabilities exist allowing intelligence agencies to intercept satellite communications.[136][137]

Crucially, by intercepting communications in this way, the communication is being interfered with within the territory of the intercepting state. This amounts to an interference with the right to privacy and must be justified according to the restrictions of human rights law. Such an interference invokes the negative obligation and responsibility of the interfering State not to violate fundamental rights.

---

[134] NSA slides explain the PRISM data-collection program, The Washington Post, June 6, 2013, Updated July 10, 2013, available at: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/; see also, Temporary Committee of the European Parliament on the ECHELON Interception System, *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*, tabled in the European Parliament on 11 July 2001.

[135] GCHQ taps fibre-optic cables for secret access to world's communications, The Guardian, 21 June 2013, available at: http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[136] The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition, Duncan Campbell, Oct 1999 http://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf

[137] Secret Power, Nicky Hager, 1996, http://www.nickyhager.info/ebook-of-secret-power/

Regardless of their location or nationality, all individuals are entitled to have their right to privacy respected not only by the State upon whose territory they stand, but by the State within whose territory their rights are exercised. If their communications pass through the territory of another State, and that State interferes with the communications, it will activate that State's jurisdiction under international human rights law. Accordingly, the US and UK owe the same obligation to each individual whose communications pass through their territory: not to interfere with those communications, subject to permissible limitations established under international law. Such "interference-based jurisdiction" obligations extend globally, regardless of boundaries.

Five Eyes legal frameworks that circumvent human rights obligations

Each of the Five Eyes members have complex legal frameworks governing the interception, monitoring and retention of communications content and data. This paper does not attempt to comprehensively outline such frameworks, and only excerpts some relevant provisions to illustrate the obfuscatory nature of legal frameworks that enable the rights of non-nationals or those outside the territory to be diminished.

United States
FISA section 1881a is entitled "Procedures for targeting certain persons outside the United States other than United States persons".

Section 1881(a) ss (a) provides:

> (a) the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

An authorisation pursuant to FISA section 1881(a) permits "foreign intelligence information" to be obtained both by directly intercepting communications during transmission and by making a request to an electronic service provider that stores the information to make it available to the authorities.

United Kingdom
The Regulation of Investigatory Powers Act 2000 distinguishes between "internal" and "external" surveillance. Where the communication is internal (i.e. neither sent nor received outside the British Islands, see RIPA s 20), a warrant to permit lawful interception must describe one person as the "interception subject" (s 8(1)(a)) or identify a "single set of premises" for which the interception is to take place (s 8(1)(b)). The warrant must set out "the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted" (s 8(2)).

Where the communication is "external", that is either sent or received outside the British Islands, RIPA s 8(1) and 8(2) do not apply. There is no need to identify any particular person who is to be subject of the interception or a particular address that will be

targeted.

New Zealand
The Government Security Communications Bureau (GCSB) is permitted to conduct interception by applying for an interception warrant under s15A of the Government Communications Security Bureau Act 2003 (amended 2013). However, s14 of the Act (as amended) states that in performing the function of intelligence gathering and analysis, the GSCB cannot "authorise or do anything for the purpose of intercepting the private communications of a person who is a New Zealand citizen or a permanent resident of New Zealand, unless (and to the extent that) the person comes within the definition of foreign person or foreign organisation....".

However, this limitation does not apply to the GCSB's two other functions – surveillance of New Zealanders related to cyber-security and assisting other agencies (such as the Police) – and the definition of "private communications" could be interpret to exclude meta-data.

Australia
Under the *Intelligence Services Act 2001*, the Australian intelligence agencies can conduct any activity connected with their functions[138] provided they have the authorisation of the relevant Minister (s8).

However, where there is an Australian person involved the Minister must be satisfied of the following before making an authorisation (s9):

(a) any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned; and
(b) there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency; and
(c) there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out.

In addition, the Minister must (s9(1A))

(a) be satisfied that the Australian person mentioned in that subparagraph is, or is likely to be, involved in one or more of the following activities:
    (i) activities that present a significant risk to a person's safety;
    (ii) acting for, or on behalf of, a foreign power;
    (iii) activities that are, or are likely to be, a threat to security;
    (iv) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and

[138] Which include to obtain foreign intelligence (ASIS), to obtain intelligence relevant to security (ASIO), to obtain foreign intelligence using the electrical, magnetic or acoustic energy (ASD), or to obtain geospatial and imagery intelligence via electromagnetic spectrum (DIGO)

Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
(v) committing a serious crime by moving money, goods or people;
(vi) committing a serious crime by using or transferring intellectual property;
(vii) committing a serious crime by transmitting data or signals by means of guided and/or unguided electromagnetic energy; and

(b) if the Australian person is, or is likely to be, involved in an activity or activities that are, or are likely to be, a threat to security (whether or not covered by another subparagraph of paragraph (a) in addition to subparagraph (a)(iii))—obtain the agreement of the Minister responsible for administering the *Australian Security Intelligence Organisation Act 1979*.

There are separate *Rules to Protect the Privacy of Australians* for each of the intelligence agencies, stating that where it is not clear whether a person is an Australian, it is presumed that a person within Australia is Australian and outside of Australia is not Australian (Rule 1.1). Where an intelligence agency does retain intelligence information concerning an Australian person, the agency must ensure the information is protected by security safeguards, and access to the information is only to be provided to persons who require it (Rule 2.2).

Canada

The *National Defence Act* pertains to the Communications Security Establishment Canada (CSEC) and establishes that the mandate of CSEC is (s273.64 (1))

(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; […]

Para (2) of the section provides that activities

(a) shall not be directed at Canadians or any person in Canada; and
(b) shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

It is evident that the legal frameworks of the Five Eyes States currently distinguish between the obligations owed to nationals or those within the States' territories, and non-nationals and those outside. In doing so, these legal frameworks infringe upon the rights of all individuals within the respective States' jurisdiction (i.e. anyone whose communications pass through and are interfered with within the territory of that State) to enjoy human rights protections equally and without discrimination.

In human rights law, discrimination constitutes any distinction, exclusion, restriction or preference, or other differential treatment based on any ground, including national or social origin, or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment, or exercise by all persons, on an equal footing, of

all rights and freedoms. The Human Rights Committee has deemed nationality a ground of "other status" with respect of article 2(1) of the ICCPR in *Gueye and ors v France*.[139]

It is both irrational and contrary to the spirit and purpose of international human rights norms to suppose that the privacy of a person's communications could be accorded different legal weight according to their nationality or residence. An equivalent distinction on the basis of ethnicity or gender would be deemed to be manifestly incompatible with human rights law; why then should States be able to purport to offer varying protections based on an individual's nationality or location? If an individual within a State's jurisdiction is granted lower or diminished human rights protections – or indeed is deprived of such protections – solely on the basis of their nationality or location, this will not only lead to a violation of the right they seek to enjoy, but will amounts to an interference with their right to be free from discrimination.

Towards an understanding of interference-based jurisdiction

Individuals have a legitimate expectation that their human rights will be respected not only by the State upon whose territory they stand, but by the State within whose territory their rights are exercised. The current legal frameworks of the Five Eyes States purport to discriminate between the rights and obligations owed to nationals or those physically within their territory, and those outside of it, or non-nationals. Yet the concept of jurisdiction, under human rights law, is not a rigid one. States have interference-based jurisdiction for particular negative human rights obligations when the interference with the right occurs within their territory. The way the global communications infrastructure is built requires that the right to privacy of communications can be exercised globally, and communications can be monitored in a place far from the location of the individual to whom they belong. Accordingly, the States Parties to the Five Eyes arrangement have jurisdiction over – and thus owe obligations to – individuals whose communications they monitor, which jurisdiction is invoked when the State interferes with the communication of an individual, thus infringing upon their right to privacy.

This understanding of jurisdiction and human rights obligations pertaining to the right to privacy is key to ensuring that individuals can seek redress against global surveillance arrangements that are threatening their rights to privacy and free expression.

[139] Gueye and Others v. France (Comm. No. 196/1985)