The NSA's New SIGINT Annex

David S. Kris*

On January 13, 2021, the National Security Agency (NSA) released a redacted version of new internal guidance designed to regulate signals intelligence (SIGINT) activity that implicates U.S. persons' privacy and the Fourth Amendment to the U.S. Constitution. The NSA is part of the Department of Defense (DOD), and the new guidance is in the form of an annex to the manual of rules governing all DOD elements, DOD Manual 5240.01, which was last revised on August 8, 2016 (DOD Manual). The official title of the new NSA guidance is DOD Manual S-5240.01-A, but I will refer to it here as the "SIGINT Annex" to the DOD Manual (and cite it as "SA"). Both the DOD Manual and the SIGINT Annex were promulgated under the authority of Section 2.3 of Executive Order 12333, which provides that "[e]lements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures" established by the head of the relevant agency with the approval of the Attorney General (AG) after consultation with the Director of National Intelligence (DNI).

The new SIGINT Annex replaces the prior NSA annex, last significantly updated on May 27, 1988, which is available in redacted form beginning on page 118 of this document (Prior Annex). At least three other internal procedures have also been superseded, as described on page 40 of the SIGINT Annex. But three additional sets of pre-existing procedures remain in effect (although they may be modified in the near future). The first of these, governing the availability of raw (unminimized) SIGINT, was approved on January 3, 2017 and is available here (Raw SIGINT Guidelines). Also relevant and still in effect are NSA's internal procedures for implementing Presidential Policy Directive 28 (January 17, 2014), issued on January 12, 2015 and available here (PPD-28 Procedures). Finally, United States Signals Intelligence Directive 18, last significantly revised on January 25, 2011 and available here (USSID 18), officially remains in force, although it is subordinate to the SIGINT Annex and a revision of USSID-18 is currently in process. In addition, the Privacy Act, 5 U.S.C. § 552a, governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. See DOD Procedure 5400.11 and GNSA-18. Together, the SIGINT Annex and these materials make up the most important elements of the publicly available, general regulatory framework currently governing SIGINT activities that implicate the privacy interests of U.S. persons, with the SIGINT Annex, the DOD Manual, and USSID-18 likely being the most important on an everyday basis. Section 6.2 of the SIGINT Annex itself requires the development and issuance of even more granular, internal operating procedures, which

---

* I have been a member of the NSA's Emerging Technologies Panel, see 50 U.S.C. § 3617, also known as the NSA Advisory Board (NSAAB) and several of its subsidiary panels. Although I consulted with officials from NSA and other government agencies regarding the accuracy of this paper, and I am grateful for the assistance they were permitted to provide, the views expressed are solely my own, and errors solely my responsibility. The SIGINT Annex is largely unclassified, and this paper is based exclusively on its unclassified portions; it was reviewed by the government to ensure that it does not contain classified information.

presumably will be classified, at least in part, and/or could be included in the forthcoming, revised version of USSID-18.

This paper reviews and analyzes the new SIGINT Annex, reading it in context with the Raw SIGINT Guidelines, the PPD-28 Procedures, and the current version of USSID-18, and occasionally comparing it to the DOD Manual, the Prior Annex, and a corresponding set of internal procedures issued in 2017 by the Central Intelligence Agency (CIA) (which I previously analyzed here).

Part I of the paper describes the origins and evolution of the SIGINT mission of the NSA and the U.S. Signals Intelligence System (USSS), which includes military SIGINT elements. It begins (I.A) before NSA's existence, in the era of telegraph wiretapping, and then follows the agency from its creation in 1952 (I.B), through the abuses of intelligence revealed in the 1970s (I.C), the aftermath of the 9/11 terrorist attacks (I.D), and the challenges of the present day (I.E). Part I also includes a discussion of SIGINT tradecraft (I.F), in an effort to explain (albeit in an unclassified manner) the operational reality of modern SIGINT collection and related work that the Annex regulates. Part I concludes (I.G) with a discussion of the main forms of SIGINT regulation. Part I is meant to provide background and context for understanding the SIGINT Annex.

Part II reviews the SIGINT Annex. It begins (II.A) with an executive summary that reviews the seven parts of the Annex and highlights major changes as compared to the Prior Annex. For those seeking a (relatively) quick review of the SIGINT Annex, reading this introduction and Part II.A (and perhaps also Part III, the Conclusion) probably will suffice. The remainder of Part II is spent on a detailed review of the SIGINT Annex (II.B), including its general provisions (II.B.1) as well as its regulation of collection (II.B.2), processing and querying (II.B.3), retention (II.B.4), and dissemination (II.B.5). Part II also covers the Annex's approach to policy, compliance, training, and auditing (II.B.6), and the rules governing collection targeting U.S. persons abroad (II.B.7). Part III of the paper is a conclusion that assesses the approach of the SIGINT Annex and summarizes its protections for U.S. persons and persons in the United States, and its protections for all persons, including non-U.S. persons located abroad.

The SIGINT Annex was released following the election of 2020, during a period of transition between two presidential administrations. This is not unprecedented: for example, the corresponding CIA guidelines that I previously reviewed were released on January 17, 2017, and the Raw SIGINT Guidelines cited above were approved on January 3, 2017 (other examples of Intelligence Community regulations are listed here). These sorts of documents are so difficult and complex that sometimes they can be finalized only with the benefit of the most rigid of forcing functions. Although the SIGINT Annex certainly may give rise to legitimate debate among informed observers concerning the appropriate balance between privacy and security, and like any set of rules and procedures it could be misused or misapplied in practice, I did not see anything in it that reflects a politicization of intelligence or other radical departure from a basic commitment to the paradigm of intelligence under law. As noted above, major changes from the Prior Annex are discussed in Part II.A.2 and throughout Part II.B.

I. HISTORY OF THE NSA'S SIGINT MISSION

A. Before NSA

Prior to the creation of NSA, the U.S. military generally controlled the U.S. Communications Intelligence (COMINT) effort. Thomas L. Burns, *The Quest for Cryptologic Centralization and the Establishment of NSA: 1940-1952* at 5 (2005) [hereinafter *Centralization*]. In the U.S. Civil War and World War I, interception focused on visual signals, telegrams sent by wire, and Morse Code radio transmissions, in keeping with the technology of the day. See Church Report Volume 5 at 6 [hereinafter *Volume 5*]; Church Report Book III at 736 [hereinafter *Book III*]. Beginning no later than the 1920s or 1930s, "elements of the [U.S.] military establishment [were] assigned tasks to obtain intelligence from foreign radio transmissions." *Volume 5* at 6. In particular, the Army and Navy both engaged in such interception, and often competed against one another but were sometimes able to work together. *Centralization* at 5-9.

Prior to World War II, the Army and Navy monitored their Axis military counterparts but competed for coverage of diplomatic traffic, focused on German, Italian, Mexican, South American, Japanese, and Soviet targets. *Centralization* at 7. Over the course of years of wartime negotiations, the two services were unable to resolve their differences and work efficiently together. For example, one interim approach, adopted in August 1940, divided coverage of Japanese diplomatic traffic so that the Army was responsible for decryption, translation and reporting on even days of the month, and the Navy was responsible on odd days. *Centralization* at 8. As a later historical account observed, "alternating the responsibility for reporting greatly increased the risk of error, duplication, and omission." *Centralization* at 8.

In the aftermath of the attack on Pearl Harbor, the Navy found itself very busy with operational naval COMINT issues, and so in 1942 it agreed to transfer responsibility for all diplomatic COMINT to the Army. *Centralization* at 7-9. At the request of GEN Marshall and ADM King, the Federal Communications Commission and Office of Strategic Services (the CIA's predecessor) were restricted by presidential order from engaging in COMINT for security reasons; the Army and Navy were concerned about leaks if too many agencies were doing COMINT or even had access to it. This resulted in the exclusion of the FCC, OSS, and other agencies from COMINT, although the FBI remained involved. *Centralization* at 11. Additional agreements between the two military services followed in 1944, but overall "each service operated with little consideration for the parallel activities and interests of the other," such that, for example, the Army and Navy established separate technical agreements with the British "without coordination or dialogue with the other U.S. service." *Centralization* at 16. The Joint Chiefs of Staff became the default coordinator between them. *Centralization* at 16.

After World War II, under pressure to reduce military spending and due to the investigation into the attack on Pearl Harbor, "[f]or the first time, U.S. intelligence operations came under outside scrutiny." *Centralization* at 25. These factors led the Army and Navy to

"support[] a merger of the COMINT services," *Centralization* at 28, and under the leadership of GEN Eisenhower and ADM Nimitz, there was a move towards more coordination, including governmental (rather than service-level) agreements with the British, *Centralization* at 30-31. (Documents pertaining to US-UK agreements between 1940 and 1961 are available here.)

In 1946, the U.S. Communication Intelligence Board (USCIB) was chartered, including representatives of the Army, Navy, and (after a request from J. Edgar Hoover) the FBI, as well as the Director of Central Intelligence (who was then the head of the Central Intelligence Group). *Centralization* at 34. The National Security Act of 1947, which among other things created the Air Force, the CIA, and the National Security Council (NSC), complicated matters. The USCIB received a charter from the NSC in 1948, in the form of National Security Council Intelligence Directive No. 9 (NSCID 9), formally making it subject to national rather than military supervision. Civilian agencies, including the FBI and State, were at various times part of the USCIB, although the military services still dominated, in part because each service had more than one representative, and hence more than one vote, on the Board. *Id*. at 37.

Infighting continued, and the USCIB spent many hours in the late 1940s deliberating over such matters as whether its role would be to provide "authoritative coordination" rather than "unified direction" to its members concerning COMINT. *Centralization* at 44. Various other structures and approaches were attempted, including the creation in 1949 of the Armed Forces Security Agency (AFSA) through Joint Chiefs of Staff (JCS) Directive 2010, *Centralization* at 49, 56-57, but AFSA failed to centralize the COMINT effort and continued to marginalize civilian COMINT agencies.

By "1951 it was clear to the civilian agencies that the military organizations were incapable of jointly developing a structure that would meet, without bias, the needs of the growing United States intelligence community. After six years of experimentation and reorganization and two attempts to consolidate and centralize the communications intelligence activities of the United States, instability, disunity, and decentralization still existed." *Centralization* at 99. In other words, "[t]he major players of the intelligence community were locked in a struggle over 'who was in charge' and over the acquisition of expanded responsibilities and authorities. The military and civilian agencies continued to argue over basic jurisdictional and organizational relationships." *Centralization* at 81-82.

Against this background, the Department of State and the CIA together persuaded President Truman in December 1951 to approve a survey of U.S. COMINT structures, which ultimately led to creation of the Brownell Committee, headed by George Brownell, a well-respected lawyer from New York (sometimes confused with Herbert Brownell, who the following year would begin a term of service as Attorney General of the United States). The Brownell Committee included representatives from the civilian intelligence agencies, such as CIA and the State Department (including a young Lloyd Cutler, future White House Counsel to Presidents Carter and Clinton), but it did not include representatives of the uniformed services. *Centralization* at 83-87, 98-99. This omission of uniformed personnel "caused great alarm within the military, particularly in the JCS." *Centralization* at 81. Nonetheless, the Committee

went forward and its report "emphasized the need for the establishment of one organization to manage the communications intelligence activities of the government" and "provided a strong indictment of service unification as it existed under AFSA." *Centralization* at 81. The Brownell Committee's work led directly to the creation of NSA (a brief and interesting note from the State Department's historians on the Committee is available here).

B. Creation of NSA

The NSA was officially conceived on October 24, 1952 through a presidential memorandum issued by Harry Truman, entitled "Communications Intelligence Activities" [hereinafter *Truman Memo*], which began with a preface noting that the "communications intelligence (COMINT) activities of the United States are a national responsibility," meaning not solely a military responsibility. The memo explained that "the terms 'communications intelligence' or 'COMINT' shall be construed to mean all procedures and methods used in the interception of communications other than foreign press and propaganda broadcasts [as to which, see my prior paper on the CIA] and the obtaining of information from such communications by other than the intended recipients, but shall exclude censorship and the production and dissemination of finished intelligence" *Truman Memo* 2.b (footnote omitted).

President Truman's memo took a circuitous route to creating NSA. It directed the Secretaries of State and Defense to form a "Special Committee of the National Security Council for COMINT, which Committee shall, with the assistance of the Director of Central Intelligence, establish policies governing COMINT activities." *Truman Memo* preface. The Special Committee was told to "prepare and issue directives," including a directive to the Secretary of Defense (a member of the Special Committee) concerning the NSA. *Truman Memo* preface. And the President, in his memorandum to the Special Committee, laid out the major elements of the forthcoming directive concerning NSA. As DIRNSA Lew Allen explained in 1975, President Truman "issued in October 1952 a Presidential memorandum outlining in detail how communications intelligence activities were to be conducted, designated the Secretary of Defense to be his executive agent in these matters, directed the establishment of the NSA, and outlined the missions and functions to be performed by the NSA." *Volume 5* at 7.

First, the President specified, the Special Committee's directive must define the NSA's "COMINT mission," which was "to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments, [and] to provide for integrated operational policies and procedures pertaining thereto." *Truman Memo* 2.b. Indeed, the President specified five "[s]pecific responsibilities" for NSA (*Truman Memo* 2.e):

> (1) Formulating necessary operational plans and policies for the conduct of the U.S. COMINT activities.

(2) Conducting COMINT activities, including research and development, as required to meet the needs of the departments and agencies which are authorized to receive the products of COMINT.

(3) Determining, and submitting to appropriate authorities, requirements for logistic support for the conduct of COMINT activities, together with specific recommendations as to what each of the responsible departments and agencies of the Government should supply.

(4) Within NSA's field of authorized operations prescribing requisite security regulations covering operating practices, including the transmission, handling and distribution of COMINT material within and among the COMINT elements under [NSA's] operational or technical contro[l]; and exercising the necessary monitoring and supervisory control, including inspections if necessary, to ensure compliance with the regulations.

(5) Subject to the authorities granted the Director of Central Intelligence under NSCID No. 5 [available here], conducting all liaison on COMINT matters with foreign governmental communications intelligence agencies.

Second, the President ordered, the Special Committee's directive must provide that "NSA shall be administered by a Director [DIRNSA], designated by the Secretary of Defense after consultation with the Joint Chiefs of Staff," who would be "responsible for accomplishing the mission of NSA." *Truman Memo* 2.c. The NSA Director would "serve for a minimum term of 4 years … be eligible for reappointment …. be a career commissioned officer of the armed services on active or reactivated status, and … enjoy at least 3-star rank during the period of his incumbency." *Truman Memo* 2.c. He would have "a civilian deputy whose primary responsibility shall be to ensure the mobilization and effective employment of the best available human and scientific resources in the field of cryptologic research and development." *Truman Memo* 2.i.

To allow for DIRNSA's success, "all COMINT collection and production resources of the United States [were] placed under his operational and technical control." *Truman Memo* 2.d. Although DIRNSA would normally operate through the leaders of agencies that contained such resources, "due to the unique technical character of COMINT operations" he was "authorized to issue direct to any operating elements under his operational control task assignments and pertinent instructions," and could have "direct access to, and direct communication with," such elements, whether military or civilian. *Truman Memo* 2.d. DIRNSA would be empowered to "centralize or consolidate the performance of COMINT functions for which he is responsible." *Truman Memo* 2.f. Where necessary, DIRNSA could delegate to military commanders "direct operational control of specified COMINT facilities and resources." *Truman Memo* 2.f.

The Special Committee was also directed to issue a replacement for NSCID 9, which (as noted above) governed communications intelligence. *Truman Memo* 1. The new version of NSCID 9 would re-charter the USCIB as a kind of high-level NSC coordinating committee for

COMINT, chaired by the Director of Central Intelligence and composed of representatives of the Secretaries of State and Defense, each of the uniformed military services, and the CIA, as well as the Director of the FBI (who had withdrawn from the Board in 1947) and the new Director of NSA. *Truman Memo* 1.b; see *Centralization* at 43. The USCIB was to operate under the supervision of the NSC Special Committee. *Truman Memo* 1.a. Its primary job was to "advise and make recommendations to the Secretary of Defense … with respect to any matter relating to communications intelligence which falls within the jurisdiction of the Director of NSA." *Truman Memo* 1.d. It also coordinated COMINT activities outside NSA's jurisdiction. *Truman Memo* 1.e. The new version of NSCID 9 was in fact issued on the same day as the President's memo and tracks it very closely. *Centralization* at 90. (A version of NSCID 9 dated December 29, 1952, with an explanation of changes made to the prior October 24 version, is available here.)

Reproduced in a publicly available glossy brochure celebrating NSA's 60th Anniversary is a DOD "disposition form," marked top secret and dated October 31, 1952, observing that "National Security Council Intelligence Directive Number 9 (revised), 24 October 1952 authorizes the replacement of the present Armed Forces Security Agency by a National Security Agency." NSA, *60th Anniversary Brochure* (2012) (hereinafter *60th Anniversary Brochure*). The NSA officially came into existence on November 4 through a "remarkably sparse announcement" from the Secretary of Defense, "Interim Implementation of NSCID No. 9 Revised." *Centralization* 90; see James Bamford, *The Puzzle Palace* at 1 (1982); Report on Special Subcommittee on Defense Agencies, House Committee on Armed Services, 87th Cong. 2d Sess. 6596 (Aug. 13, 1962) [hereinafter *1962 Armed Services Report*]. A month later, on December 5, the Secretary of Defense sent a superseding memo, without the word "Interim" in its title, announcing that the "National Security Agency (NSA) is hereby established as an agency within the framework of the Department of Defense."

The "very existence of … NSA … was not acknowledged until 1957," Church Report Book I at 24, and efforts by Congressional overseers to understand NSA as late as the mid-1970s are somewhere between tragic and comic. As the agency's extremely capable and helpful historian put it, "NSA did appear on some charts and in the Pentagon phone book, but the text describing us was so vanilla as to be useless to any readers who did not already have guilty knowledge." NSA's own 60th Anniversary brochure explains that "[f]rom its inception, NSA had developed what could only be described as a cursory relationship with the U.S. Congress." *60th Anniversary Brochure* at 54. Nonetheless, in 1959 Congress enacted the National Security Agency Act, Pub. L. No. 86-36, 73 Stat. 63, which provides for the nomination and confirmation of DIRNSA, among other things. See 50 U.S.C. § 3602. Testifying in 1975, DIRNSA Lew Allen argued that in "1962 a Special Subcommittee on Defense Agencies of the House Armed Services Committee concluded, after examining the circumstances leading to the creation of defense agencies, that the Secretary of Defense had the legal authority to establish the National Security Agency." *Volume 5* at 7 (the 1962 report, available here, identifies concerns with the creation of two defense agencies, not including NSA). The first public speech by an NSA Director (ADM Inman) was not given until 1979. Thomas R. Johnson, American Cryptology During the Cold War, 1945-1989, Book III: Retrenchment and Reform, 1972-1980 (1998) [hereinafter *Retrenchment and Reform*] at 238.

As explained in an official NSA historical report, the October 24 memo from President Truman was "an extraordinary directive that changed the organization and direction of the U.S. communications intelligence structure and laid the policy framework for the modern system":

> Truman stated that the communications intelligence function was a national responsibility rather than one of purely military orientation. This triggered actions that reorganized the U.S. military COMINT effort and strengthened the COMINT roles of the USCIB and the NSC and brought a wider role for the civilian agencies in U.S. COMINT operations. The president's memorandum also contained the first reference to a "National Security Agency," to be established in place of the Armed Forces Security Agency. Under Truman's directive, the Department of Defense became the executive agent of the government for the production of communications intelligence information, thereby removing the JCS [Joint Chiefs of Staff] as the controlling authority for the COMINT process.

Centralization 81.

The first DIRNSA, General Ralph Canine, gave a speech to the new NSA workforce on November 25, 1952, in which he provided his perspective on President Truman's memo:

> Mr. Truman did one very critical, crucial thing. He took all the Comint collection and production resources of the United States and placed them under the Director of the National Security Agency. By that means he then made the Director responsible for carrying out the national mission of the National Security Agency. In other words, by that manipulation they succeeded in pinning down the responsibility for the conduct of all communications intelligence activities in one guy so that they only got one neck to chop off, one guy to go up on the Hill when the next Pearl Harbor comes along. Well, that's simple for them, but I doubt that's just exactly why they did it. They can have my neck, if they want it, or whomever happens to be unfortunate enough to be Director at that particular time, but they have succeeded in pin-pointing responsibility and in tremendously increasing that responsibility of the Director and his assistants.

General Canine also candidly acknowledged the controversial nature of the President's decision, particularly for employees who, a few weeks earlier, had been part of the military's AFSA (ellipsis in original):

> Now not everybody in the United States approves what has been done. That's probably an understatement.... Some very bitter words have been passed back and forth over the Comint racket at one time or another.... Some of you people in here ... have had one gob of these diverse opinions. Some of you have been on the other side and I suppose some of you have been in the middle. Some of you have been rather vocal about your opinions, maybe before you came to this Agency. Some of you had very fixed ideas. Well, that's water over the dam. You may have had them yesterday, but you haven't got

them today. I mean that exactly. We've got something that's the law of the land, that's signed by the President of the United States and yesterday was yesterday. Tomorrow is tomorrow. We have got a lot of work to do here.

So much for the chronology of the beginnings of the predecessors of the National Security Agency in our present position.

Today, even after NSA21, the latest reorganization of the agency launched in 2016, President Truman's description of NSA, and General Canine's recognition of the hybrid nature of the agency, both remain relevant (although NSA's organizational chart, which is protected from disclosure under 50 U.S.C. § 3065, presumably has evolved in complexity from earlier versions that are available here and here). As of 2016, the major NSA Directorates were Workforce Support Activities; Business Management & Acquisition; Engagement and Policy; Operations; Capabilities; and Research. In 2019, NSA created a new Cybersecurity Directorate.

By statute, DIRNSA is nominated by the President and confirmed by the Senate, 50 U.S.C. § 3602, and the Secretary of Defense must consult with the Director of National Intelligence before recommending a nominee to the President, 10 U.S.C. § 201; 50 U.S.C. § 3041. By regulation, NSA continues to have a military leader, who "shall enjoy not less than three-star rank during the period of incumbency," with a deputy who must be a "career civilian with cryptologic experience." DOD Directive 5100.20 § 9(a)-(b) (originally issued in 1959) (hereinafter DOD 5100.20]. Today, the Director of NSA is also the commander of Cyber Command, and so enjoys four-star rank. If NSA and Cyber Command are split – a possibility that has been under consideration in one form or another for years – it may be that the successor DIRNSA will be a civilian, which would extend the evolution of signals intelligence (SIGINT) away from its military origins. A good primer on NSA's basic organization and structure, prepared for the Presidential Transition Team in late 2016, is available here.

By executive order, DIRNSA is the nation's functional manager for SIGINT, EO 12333 § 1.3(b)(12)(A)(i), and has several other specific responsibilities, such as collecting, processing, analyzing, producing and disseminating SIGINT, EO 12333 § 1.7(c). "No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director." EO 12333 § 1.7(c)(2). In particular, under Section 1.7(c) of Executive Order 12333, the "Director of the National Security Agency shall:"

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions.

(2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other

department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

(3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;

(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

NSA's mission is to serve as "the U.S. Government (USG) lead for cryptology, and its mission encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) activities." DOD 5100.20 § 4. It "provides SIGINT and IA guidance and assistance to the DoD Components, as well as national customers," and DIRNSA "serves as the principal SIGINT and IA advisor to the Secretary of Defense" and various other DOD officials, the Chairman of the JCS and various other service leaders, "and the DNI, as well as other USG officials with regard to these missions and the responsibilities enumerated herein." DOD 5100.20 § 4. NSA is both a "Combat Support Agency of the Department of Defense" and "an element of the Intelligence Community (IC) subject to the oversight of the DNI." DOD 5100.20 § (5)(b) & (e). Today, and in keeping with instructions applicable to DOD in general, NSA has largely re-branded its IA mission as a "cybersecurity" mission, touting the synergies between cybersecurity and SIGINT ("Our foreign intelligence mission enhances our cybersecurity mission with key insights. We have practical experience with the ways adversaries exploit networks, and what is truly effective in thwarting intruders. We can also inform defenses as we see hostile foreign powers develop cyber capabilities and operate.").

C. Abuses and Retrenchment

Beginning soon after it came into existence, NSA engaged in violations of Americans' privacy rights. Many of these are documented in great detail in Volume 5 and Book III of the Church Committee's Report, which focused on three problematic programs. "The Committee's hearings disclosed three NSA interception programs: the 'watch lists' containing names of American citizens [including under the codename MINARET]; 'Operation SHAMROCK,' whereby NSA received copies of millions of telegrams leaving or transiting the United States; and the monitoring of certain telephone links between the United States and South America at the request of the Bureau of Narcotics and Dangerous Drugs" (BNDD), the predecessor of today's Drug Enforcement Administration (DEA). *Book III* at 738. (For an internal NSA historical study of this period, now declassified, see pages 83-88 and 91-100 of *Retrenchment and Reform*.)

1. SHAMROCK

For 30 years, from the end of World War II until May 1975, NSA "received copies of millions of international telegrams sent to, from, or transiting the United States." *Book III* at 740. (No domestic telegrams were reviewed by NSA as part of the program. *Book III* at 776.) As the Church Report explained, "SHAMROCK was probably the largest governmental interception program affecting Americans ever undertaken" by the U.S. government as of that time. *Book III* at 765. In the last two or three years of the 30-year project, "about 150,000 telegrams per month were reviewed by NSA analysts." *Book III* at 765. In the aftermath of World War II, the three major telegram service providers (ITT, RCA and Western Union) raised concerns about the legality of the program and were apparently told by the Secretary of Defense that the Attorney General had opined that the program was legal and that the President had approved it. The chairmen of the House and Senate Judiciary Committees were briefed and advised that Section 605 of the Communications Act, 47 U.S.C. § 605, should be amended to more explicitly allow for the program. *Book III* at 769-770. An amendment to that effect was approved in executive session by the Senate Judiciary Committee, but not unanimously, and a decision was made not to bring the bill to the floor for debate, presumably due to fear of disclosure. *Book III* at 770. A subsequent Secretary of Defense in 1949 gave the companies the same assurances of legality and Presidential approval. *Book III* at 770. It does not appear that further assurances were sought or provided. *Volume 5* at 59.

Initially, paper telegrams were reviewed by hand; but beginning in the mid-1960s, the companies began providing telegrams on magnetic tape. "This was significant because it meant that the telegrams of citizens whose names were on NSA's 'watch list' could be selected for processing by NSA analysts." *Book III* at 775. The program was terminated in 1975, by order of the Secretary of Defense, officially "because (1) it was no longer a valuable source of foreign intelligence, and (2) the risk of its exposure had increased." *Book III* at 776.

2. MINARET

As described in the Church Report, from "the early 1960s until 1973, NSA intercepted and disseminated international voice communications of selected American citizens and groups on the basis of lists of names supplied by other Government agencies. In 1967, as part of a general concern within the intelligence community over civil disturbances and peace demonstrations, NSA responded to Defense Department requests by expanding its watch list program. Watch lists came to include the names of individuals, groups, and organizations involved in domestic antiwar and civil rights activities in an attempt to discover if there was 'foreign influence' on them." *Book III* at 739. This was expanded in 1967 and formalized in 1969 under the codename MINARET. *Book III* at 739; see *Book III* at 744-746.

The NSA charter for MINARET, issued in July 1969, covered not only "foreign governments, organizations or individuals," but also "U.S. organizations or individuals who are engaged in activities which may result in civil disturbances or otherwise subvert the national security of the U.S." It "specifically include[d] communications concerning individuals or organizations involved in civil disturbances, anti-war movements/demonstrations and military deserters involved in anti-war movements." Charter 1, 2. Given this scope and focus on domestic activity, "[a]n equally important aspect of MINARET [was] to restrict the knowledge that such information is being collected and processed by the National Security Agency." Charter 1. These communications involving Americans (initially, only communications between two Americans, but later any communication to, from, or about any one American) "were classified Top Secret, prepared with no mention of NSA as the source, and disseminated 'For Background Use Only.' No serial number was assigned to them, and they were not filed with regular communications intelligence intercepts." This limited access to the material, and probably made the reports of communications appear to be based on human intelligence (HUMINT) rather than SIGINT, and also reflected an understanding that the activity was "different from the normal mission" of NSA and perhaps outside its authorized mission. *Book III* at 747-748 (internal quotations and emphasis removed).

In 1973, the Justice Department advised NSA that MINARET was of "questionable legality," in part because it targeted domestic persons and entities. *Book III* at 739; see *Volume 5* at 160 ("The practice by NSA of conducting electronic surveillance at the request of an investigative agency [the FBI or Secret Service] and disseminating the information obtained thereby raises a number of serious legal questions which have yet to be resolved"). In response, NSA took the position that "although specific names had been targeted, the communications of particular Americans included on the watch lists had been collected 'as an incidental and unintended act in the conduct of the interception of foreign communications.'" *Book III* at 739; see *Volume 5* at 162 ("No communications intercept activities have been conducted by NSA, and no cryptologic resources have been expended solely in order to acquire messages concerning names on the Watch Lists; those messages we acquire are by-products of the foreign communications we intercept in the course of our legitimate and well recognized foreign intelligence activities"). Watchlisting activities involving U.S. citizens were discontinued in 1973. *Book III* at 744, 760-761.

This 1970s dialogue between NSA and DOJ in some ways resembles more recent debates, reflecting a distinction between *collection* of information for a foreign intelligence purpose and *querying* (and subsequent use) of collected information for a different purpose. Cf. 50 U.S.C. § 1881a(f). Watch lists, as described in the Church Committee's report, were in some ways roughly analogous to query terms, albeit apparently limited to selecting communications in real time rather than from storage due to the technology of the day: "Lists of words and phrases, including the names of individuals and groups . . . used by the National Security Agency to select information of intelligence value from intercepted communications." *Book III* at 743. NSA would receive watch lists of names from the FBI and Secret Service, add to the lists based on its own information, and then use them to extract relevant communications from ongoing collection on links or other facilities involved in communications involving at least one end outside the United States. *Book III* at 743-744. Watch lists did not expand collection to new links or facilities (with the exception of the BNDD program discussed below), which appears to be the argument at the core of NSA's defense of the program's legality in response to concerns expressed by DOJ. But Watchlisting certainly did expand retention and dissemination of information. "At its height in early 1973, there were 600 American names and 6,000 foreign names on the watch lists," which produced "about 2,000 reports . . . between 1967 and 1973," of which approximately "10 percent" were "derived from communications between two American citizens." *Book III* at 747.

3. SIGINT ON DRUG TRAFFICKING (BNDD)

In 1970, the U.S. Bureau of Narcotics and Dangerous Drugs (BNDD) "asked NSA to provide intelligence on international drug trafficking," and NSA "began to monitor certain international communications links between the United States and South America to acquire intelligence on drugs entering the United States." *Book III* at 744. This was the only instance in which NSA expanded collection to new facilities (links) for a purpose other than foreign intelligence collection. *Book III* at 744; see *Book III* at 752. The concern was that pay telephones in Grand Central Station were being used by drug dealers in the U.S. to communicate with their suppliers in South America: "BNDD felt that it could not legally tap the public telephones and thus enlisted NSA's help to cover the international link that carried these telephone calls." *Book III* at 753. At the high point of collection, "in early 1973, 250 Americans were on the active list" for selection from the traffic passing through the monitored facilities. *Book III* at 753.

The Church Report, and its fallout, and related events such as Watergate, led NSA to focus even more heavily on foreign adversaries. As one NSA historical account explains, the exposure of misconduct by NSA and other agencies created "ignominy and public suspicion of intelligence and cryptology." It also led to Executive Order 11905, issued by President Ford in 1976, which provided (§ 5(b)(2)) that "[f]oreign intelligence agencies shall not engage in . . . [e]lectronic surveillance to intercept a communication which is made from, or is intended by the sender to be received in, the United States, or directed against United States persons abroad, except lawful electronic surveillance under procedures approved by the Attorney General." This "resulted in the termination of many NSA activities in support of law

enforcement," some of which apparently remain classified. See *Retrenchment and Reform* at 105. Today, USSID 18 and the SIGINT Annex, EO 12333 and FISA together impose far more detailed restrictions. NSA generally retreated from domestic surveillance beginning in the 1970s, but continued wiretapping foreign embassies in the United States (albeit with Attorney General approval). For a survey of NSA's role in securing communications during this period, both for the government and the private sector, see Susan Landau, Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure, 7 Journal of National Security Law & Policy 411 (2014) [hereinafter *Under the Radar*] and *Retrenchment and Reform* at 142-151.

D. 9/11 Challenges

In the aftermath of the September 11, 2001 attacks, NSA had to adapt, shifting from a Cold-War focus on nation-state adversaries (chiefly, the USSR) to the asymmetric threat of international terrorist groups, and protecting the U.S. homeland from kinetic strikes. With the rise of packet-switched networks and other digital network technology, the operating environment for NSA also shifted to include more domestic infrastructure and other elements that carried domestic traffic. These two factors – changing threats and changing technology – together exerted profound effects on the operation and regulation of SIGINT. Former DIRNSA (and then CIA Director) GEN Michael Hayden explained these effects in testimony before the Senate Judiciary Committee in 2006 (page 6 of the transcript available here):

> NSA intercepts communications … to protect America … By the late 1990s, that had become increasingly difficult. The explosion of modern communications in terms of volume, variety, and velocity threatened to overwhelm us as an agency.
>
> The September 11th attacks exposed an even more critical and fundamental fault line. The laws of the United States do, and should, distinguish between the information space that is America and the rest of the planet … But modern telecommunications do not so cleanly respect that geographic distinction.

In part because the events in question are still relatively recent, and in part because I experienced or participated in many of them directly, the discussion that follows in this part and the next may reflect more of my individual perspective than the discussion of earlier periods as to which the history has had more time to settle.

The new threats and technological environment of the post-9/11 era triggered significant changes in NSA's SIGINT collection. Beginning in the fall of 2001, and proceeding at various times under unilateral executive authority, judicial approval, and legislation, NSA's SIGINT collection expanded to include programmatic, bulk, and iterative collection of communications contents and metadata from U.S. communications providers. Beginning in early October 2001, NSA at the direction of President Bush engaged in collection of both contents and metadata, including domestically and in bulk, without the approval of the FISA Court. Over time, this activity was brought under the auspices of the Court – briefly for content

collection and more enduringly for bulk metadata collection. Eventually, three new statutory authorities were enacted: the Protect America Act (PAA) for programmatic content collection between August 2007 and July 2008; the FISA Amendments Act (FAA) for such collection from July 2008 to the present; and the USA Freedom Act to restrict bulk metadata collection and replace it with a regime of iterative collection from June 2015 to March 2020. Implementation of the new authority, particularly with respect to bulk metadata collection under FISA Court supervision, was plagued by extensive and repeated compliance violations. Like a business expanding into a new market, NSA's expansion into areas more heavily regulated by FISA and other laws created problems because the agency's operational capabilities exceeded its compliance capabilities, requiring the latter to be upgraded over time.

The operational, legal, and political history of the period immediately after 9/11 has been covered extensively elsewhere and is within the memory of many of the (relatively few) individuals who will read this document. The summary above should therefore suffice. More detailed information is available in Chapters 15 and 16 of National Security Investigations and Prosecutions [hereinafter *NSIP*]; On the Bulk Collection of Tangible Things [hereinafter *Bulk Collection Paper*]; The NSA and the USA Freedom Act [hereinafter *NSA and USA Freedom*]; and various reports by Inspectors General, including an unclassified report from 2009 that is available here, and several partially declassified reports that are aggregated and available here and here. A very brief (five-paragraph) chronology of relevant events from the Office of the Director of National Intelligence (ODNI) is available here.

E. Current Issues

If post-9/11 SIGINT was informed by changing threats and technology, the current SIGINT environment reflects continued change in those two areas plus a third factor: domestic political polarization and challenges to the paradigm of apolitical intelligence under law. Recognizing and seeking to encourage that third factor, U.S. nation-state adversaries use cyber and information operations to engage in election interference and other attacks understood to be below the threshold of armed conflict. In response, U.S. SIGINT and Cyber operations are adapting through doctrines of "defend forward" and "persistent engagement" enabled by new legal and policy support, with leaders trying to protect and motivate the Intelligence Community workforce in difficult times.

A dozen years after the 9/11 attacks, as the terrorist threat was perceived to be receding, disclosures by Edward Snowden, and the reactions they provoked, exacerbated concerns about questionable surveillance practices. Morale at NSA suffered as the workforce felt the brunt of extensive outside criticism. The Obama Administration's tepid defense of the agency, and later President Trump's flamboyantly ambivalent relationship with electronic surveillance and the Intelligence Community, meant that NSA lacked a reliable supporter in the White House across two Presidential administrations.

Beginning in 2017, the Trump Administration's increasingly extraordinary behaviors required intelligence (and law enforcement) personnel to devise creative coping mechanisms,

as they struggled to integrate the required deference both to the preferences of policymakers and to the requirements of law – mandates that had not been in such tension with one another since before the reforms of the mid-1970s. After an initial period of experimenting with efforts to build capital with the President, many IC leaders appeared to pursue a heads-down approach, keeping their distance, focusing on mission, and encouraging their employees to stay submerged and ignore the surface turbulence. This probably was the best approach available under the circumstances, but its major drawback was that it tended to normalize, through the absence of comment or other acknowledgment, the extraordinary conduct at high levels of the executive branch. Ignoring turbulence of such obvious magnitude did not dispel it or its potentially damaging effects on the workforce. The long-term effects of this remain to be seen.

Technological change also continued to create significant disruption. As discussed in greater detail here, advancing digital network technology created conditions harmful to both privacy and security. These conditions included growing amounts of personal data that might be exposed to the public but also created a haystack problem for investigators looking for dangerous needles; data that were sometimes consolidated (and therefore at risk of wholesale compromise) and sometimes fragmented (and therefore not well protected or easy to find); increased cooperation between authoritarian governments and the private sector but decreased cooperation between the U.S. government and the private sector; and greater freedom of choice with respect to anti-surveillance technologies, causing bad actors to adopt measures such as strong encryption and location-masking to evade detection while ordinary persons mainly left themselves exposed. The rise of social media – Facebook and Twitter became available to the general public only in 2006, and became public companies in 2012 and 2013 – changed the way Americans and others communicated and accessed news, creating opportunities for adversary information operations as defenders struggled to catch up.

Today's Intelligence Community describes the threat environment using a "2+3" framework to embrace China and Russia, plus Iran, North Korea, and violent extremists, as described here. We are much closer to the pre-9/11 focus on nation-state adversaries, albeit a more diverse array of such adversaries, than to the nearly singular concentration on international terrorism that endured after the attacks.

The increasing emphasis on nation-state adversaries has naturally brought an increasing focus on protecting against their preferred methods, including cyber operations and misinformation and disinformation campaigns (al Qaeda did not have a very developed cyber capability and it did not engage in election interference). Here is my summary of how the Director of NSA, General Paul Nakasone, recently described the cyber threat environment within the 2+3 framework:

- "The ***Chinese government*** uses cyber capabilities to steal sensitive data, intellectual property, and personal data from the U.S. government and U.S. businesses at great cost to the U.S. economy and national security. In May 2020, the FBI and the Department of Homeland Security warned about the People's Republic of China's efforts to compromise medical research into COVID-19 vaccines. The PRC supplements those

cyberspace operations with influence campaigns to obscure international narratives about their activities." As I have written elsewhere, it may be difficult for outsiders to appreciate the centrality of China as a source of foreign policy and national security challenges for the current and any future administration.

- "***Russia*** uses cyberspace for espionage and theft and to disrupt U.S. infrastructure while attempting to erode confidence in the nation's democratic processes." Note the contrast in Nakasone's description of how and why China and Russia use influence operations ….

- "***Iran*** undertakes online influence campaigns, espionage efforts, and outright attacks against government and industrial sectors." Note here the reference to "outright attacks." Nakasone elsewhere asserts that "so much of the corrosive effects of cyber attacks against the United States occur below the threshold of traditional armed conflict." But he also warns that "much of Cyber Command's combat power had been devoted toward preparations in the event of future contingencies."

- "***North Korea*** flouts sanctions by hacking international financial networks and cryptocurrency exchanges to generate revenue that funds its weapons development activities." Here the emphasis is on revenue-generating activities for the cash-strapped regime. Nakasone heavily emphasizes interagency cooperation in cyber, discussing how the NSA and Cyber Command share information and otherwise cooperate with the Department of Homeland Security (DHS) and the FBI. He's also undoubtedly aware of the criminal charges and other legal action taken by the Department of Justice involving North Korean hackers and cyber thieves (most recently, here), as discussed here.

- Finally, Nakasone writes that "***[v]iolent extremist organizations*** have used the Internet to recruit terrorists, raise funds, direct violent attacks, and disseminate gruesome propaganda." This has been a trend from al-Qaeda's Inspire magazine and Anwar al-Awlaki's videos to the Islamic State. Nakasone touts the cyber successes the U.S. has enjoyed against the Islamic State in particular: "The terrorist group's propagandists used to spread their message on Twitter, YouTube, and their own websites. Today, because of our efforts, they have a much harder time doing so. At the height of its influence, ISIS published magazines in multiple languages, but it now struggles to publish in anything other than Arabic. At the same time as the U.S.-led coalition of conventional forces has prevailed over the physical caliphate, Cyber Command's efforts have helped defeat the virtual one."

As GEN Nakasone explained in February 2019, "I assess we are seeing what we term corrosive threats, in which malicious cyber actors weaponize personal information, steal intellectual property, and mount influence campaigns. Such measures have had and will have strategic effects on our nation and allies."

Considering these threats and technological developments, and in a period of transition between Presidential administrations, NSA today finds itself compelled to build a broader base of external support to foster partnerships, on which it increasingly depends to carry out its mission, including its increasingly vital cybersecurity mission. But it faces a polarized and volatile domestic political environment in which it must contend with sophisticated and aggressive nation-state cyber threats that require a whole-of-nation response. Those threats play out in a battle space that is largely controlled by the private sector, which enjoys arguably superior ability to access and assess data as compared to NSA itself, but at a time when U.S. public-private partnerships remain profoundly challenged, even if they have rebounded somewhat from their nadir in 2013. And NSA rightly feels compelled to develop and maintain analytic superiority using information science against foreign governments with access to very large data sets for training artificial intelligence models, no significant limits on their own surveillance and related activities, and whole-of-nation abilities facilitated by authoritarianism. (For more detail on these challenges, see here, here, and here.) This is the world in which the SIGINT Annex must function to protect both privacy and security.

F. SIGINT Tradecraft

To understand the SIGINT Annex, and the regulation of SIGINT more generally, it is important to understand something about how SIGINT is actually done. Without that understanding, the rules don't make as much sense. NSA's website has a page devoted to "Frequently Asked Questions about Signals Intelligence (SIGINT)." This SIGINT FAQ page explains that NSA "collects SIGINT from various sources, including foreign communications, radar and other electronic systems. This information is frequently in foreign languages and dialects, is protected by codes and other security measures, and involves complex technical characteristics." Here is former DIRNSA Michael Hayden's more detailed description of SIGINT in 2002:

> Thousands of times a day, our front-line employees have to answer tough questions like: Who are the communicants? Do they seem knowledgeable? Where in the conversation do key words or phrases come? What is the reaction to these words? What world and cultural events may have shaped these words? … How much of the conversation is dominated by these events and are any of the phrases tied to them?
>
> And, if you were responsible for the management (or oversight) of NSA, you would have to ask other questions like: Where was the information collected? Were any of the communicants targeted? How many calls a day are there from this location? In what languages? Hazzar? Urdu? Pashto? Uzbek? Dari? Arabic? Is there a machine that can sort these out by language for you, or do you have to use a human? If there is such a machine – does it work in a polyglot place where one conversation often comprises several languages? How long does it take NSA to process this kind of material? (After all, we are not the intended recipients of these communications). Does our current technology allow us to process it in a stream or do we have to do it in batches? When the data is processed, how do we review it – oldest to newest or newest first? And aside

> from how we normally process it, did the sequence change at 08:46 a.m. on September 11th? Without explaining the context in which SIGINT operates, unauthorized disclosures do not inform public discourse; they misshape it.

Although NSA is famously reticent about describing SIGINT, its counterpart in the UK, Government Communications Headquarters (GCHQ), has been more forthcoming. Indeed, in 2020, a Canadian professor, John Ferris, published an authorized history of GCHQ, *Behind the Enigma*, including a foreword by the agency's director. Professor Ferris assessed (page 3) that history is valuable both to GCHQ itself – as an enhancement of its institutional memory – and to outsiders trying to understand and support the agency's mission:

> The secrecy which surrounded its history hampered GCHQ's work by denying it an informed understanding of how Sigint functioned. During the Korean war, for example, Anglo-American Siginters forgot matters of tactical support they had mastered just a few years before. Siginters did not know how and why their work had mattered. Armies, conversely, believed that all officers needed a critical and thorough grasp of military history. From 2000, GCHQ debated the need to reshape the balance between secrecy and openness. It recognized the public demand to know more about work done in their name, and thought itself misunderstood and under-appreciated, yet with a good story to tell … Public trust in GCHQ remains high. Secrecy, while essential to operations, inculcates both glamour and suspicion.

This assessment of the value of transparency to GCHQ might profitably be applied to NSA today. In a podcast that I recorded with two former members of GCHQ in December 2020, we discussed the role of the GCHQ historian as a public spokesperson for the agency and the importance of transparency in building public support and trust. We also covered the importance of SIGINT for the UK in both WWI and WWII.

GCHQ has tried to describe the value of SIGINT concretely by answering in an online publication the specific question, How does an analyst catch a terrorist?. This publication asks readers to imagine that a British HUMINT source based overseas

> has seen an individual (whom we'll call the facilitator), known to be a member of ISIL leadership (Islamic State in Iraq and the Levant), passing an envelope containing pages of handwritten Arabic text to a stranger along with the message that it contained "information for the brothers in the United Kingdom that will cause carnage across London".

Unfortunately, the source reports that "all he knows about the stranger is that he spoke in English as well as Arabic. The stranger had a mobile phone – nothing fancy – and a tablet, which the source recognised as being a fairly new model of a high-end brand."

Armed with this information, the SIGINTers at GCHQ go to work. It turns out that the ISIL facilitator is known at Cheltenham, and while the analysts haven't seen or heard anything about

the envelope or the mysterious stranger, they obtain authorization to query their data repositories and review the facilitator's call detail records by recording a justification of this sort: "This number has been used previously by a known ISIL facilitator. Search is in order to identify an unknown contact who is suspected of being involved with a terrorist plot in the UK."

The analysts also attack the problem from the other direction, looking for the stranger's "nothing special" telephone. Using their expert tradecraft in ways not described in detail by GCHQ, "One candidate telephone is found. The pattern of calls it has made are consistent with how we believe the stranger is likely to have behaved. What do we do next to confirm or dismiss this lead?" They decide to consider the fancy tablet:

> Using additional data-mining techniques we can identify activity on the internet that might relate to the stranger's tablet. For each query we must supply a justification as outlined previously.
>
> The results show twenty one tablets fit our theory. This is still too many to work with. But comparing what we know about the tablet and the telephone suggests that one is of particular interest. [Perhaps, for example, both the phone and the tablet are used at the same time from the same location.] A coincidence perhaps, or evidence that the suspect phone and tablet are connected.

The story continues as GCHQ begins to zero in on the user of the fancy tablet: "Looking at the user of the tablet we have identified, we see indications of online extremist behaviours. We also spot that this individual has accessed an account for a particular internet service." Cross-referencing the internet service account against known bad guys, they find that "it has come up in connection with a previous investigation and the user has been identified. We now have a name that could belong to our stranger." In the GCHQ publication, MI-5 and MI-6 are then alerted, and Britain is saved!

In 2019, as focus shifted from terrorism to cyber threats, GCHQ allowed a journalist to spend six days inside its headquarters in Cheltenham (and in two additional facilities), and to interview 20 employees. Here are excerpts from this journalist's account, quoting GCHQ personnel:

> "Our starting point is radically different from people who work in humint …" he says. "If you work in human intelligence, you have got an individual who has access [to information]. And either because that person is venal or idealistic, you will play on that person to deliver the information you want."
>
> By contrast, GCHQ "is about understanding the technology of communications: how do they work? How might we exploit that signal? And how can we access that modem or app if we ever needed to?"

GCHQ's focus on being able to "access that modem or app if we ever need to" may be similar to current U.S. doctrine as expressed in the National Cyber Strategy and Defense Department Cyber Strategy, both released in 2018, and perhaps also in National Security Presidential Memorandum 13. The DOD Cyber Strategy expressly promotes a "defend forward" strategy that involves "leveraging our focus outward to stop threats before they reach their targets." Here is a key paragraph from the summary (emphasis in original):

> The Department must take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia. We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. We will collaborate with our interagency, industry, and international partners to advance our mutual interests.

That kind of day-to-day action and pre-positioning to gather intelligence requires speed and agility in SIGINT collection and analysis. GEN Paul Nakasone has been DIRNSA and Commander of U.S. Cyber Command since May 2018, and he explained the role and value of SIGINT from a cyber perspective in a January 2019 interview with Joint Forces Quarterly (emphasis added):

> our nation is in constant contact with its adversaries; we're not waiting for adversaries to come to us … We have to actively defend; we have to conduct reconnaissance; we have to understand where our adversary is and his capabilities; and we have to understand their intent … [W]e must operate continuously to seize and maintain the initiative in the face of persistent threats … in this domain, the advantage favors those who have initiative. If we want to have an advantage in cyberspace, we have to actively work to either improve our defenses, create new accesses, or upgrade our capabilities. This is a domain that requires constant action because we're going to get reactions from our adversary. From that reaction stems our next move … [Our adversaries] are actively in our network communications, attempting to steal data and impact our weapons systems. So advantage is gained by those who maintain a continual state of action.

On Valentine's Day 2019, GEN Nakasone testified before the Senate Armed Services Committee about efforts to secure the November 2018 mid-term elections. Again, he emphasized that "[c]yberspace is a contested environment where we are in constant contact with adversaries," including in the DOD Information Network (DODIN) and the Defense Industrial Base (DIB). Cyber adversaries, he said, "are acting and taking risks in seeking to gain advantage without escalating to armed conflict; they are conducting campaigns to gain cumulative advantage (these include theft of intellectual property and personal information, malign influence and election interference, efforts to circumvent sanctions, and probes and

positioning to threaten critical infrastructure)." To meet those challenges, Nakasone explained the focus on "defending against malicious cyberspace activities as far forward as possible," and described the work of the "Russia Small Group to protect the [2018] elections from foreign interference and influence." His view is that the "tight links between USCYBERCOM and NSA" – i.e., the tight links between SIGINT and cyber activity – "created a mutually beneficial, intelligence-operations cycle that let us rapidly find and follow leads, discover new information, and create opportunities to act in conjunction with partners."

SIGINT is distinct from cyber operations, but DIRNSA's view is that SIGINT enables and supports cyber operations, including defending forward. As Nakasone tweeted on the day of the 2020 U.S. presidential election (emphasis added), "We know our adversaries better than they know themselves. We stand ready with our partners to generate insights, enable defenses, and when authorized, impose costs on foreign adversaries. Rest assured, if called to, we will act… When you combine the insights and expertise of a preeminent cryptologic agency with the capabilities of a military combatant command, you get a powerful united effort that helps defend our Nation and secure the future." Of course, our adversaries are not without their own capabilities, as revealed publicly in late 2020 (shortly before this paper was finalized) with the SolarWinds exploit.

G. Forms and History of SIGINT Regulation

The final element of context for understanding the SIGINT Annex concerns the forms and history of SIGINT regulation. From the early days, NSA's charter was set by NSC intelligence directive – in particular, NSCID-9 and NSCID-6, issued on 15 September 1958. (A pre-NSA version of NSCID-6, dated 12 December 1947, is available here; the 1972 version of NSCID-6 is available here and portions are quoted in a 1969 memo from the CIA Director to the Secretary of Defense, and in an internal NSA brochure on ELINT.) Internal guidance was in the form of NSA directives, the first of which, NSA Directive 1, was issued on January 1, 1953. NSA itself used the Manual of U.S. Signals Intelligence Operations (MUSSO) in the 1950s, but introduced the U.S. Signals Intelligence Directive (USSID) system by issuing USSID-1 in 1970 (the current version of USSID-1, issued in 1994, is here). See *60th Anniversary Brochure* at 55. As a declassified internal NSA newsletter from 1973 explained, "We don't always do a very good job of getting good instructions to the field. Yet those instructions can make or break the Director's control of U.S. Sigint operations." Indeed, NSA from the beginning had many internal regulations, including No. 64-4, issued on April Fools' Day in in 1971 but by no means a joke, to "assign[] responsibilities for the sale and use of beer at NSA installations in the United States."

NSA is a highly regulated entity. The SIGINT Annex is subordinate to, and derived from, Executive Order 12333, which itself is a direct descendant of President Ford's Executive Order 11905, the first such order designed comprehensively to organize and limit the conduct of the U.S. Intelligence Community after disclosure of the abuses documented by the Church Committee (this paragraph and the next two are taken from my prior paper on CIA's U.S. person procedures). President Ford's order replaced NSCID-1, which had been issued in 1947 (and updated over the ensuing years), including in a 1971 memorandum on the "Organization

and Management of the U.S. Foreign Intelligence Community." Section 5 of President Ford's order, entitled "Restrictions on Intelligence Activities," observed with some understatement that "[r]ecent events have clearly indicated the desirability of government-wide direction which will ensure a proper balancing" of the government's need for foreign intelligence and "established concepts of privacy and our civil liberties." It directed each relevant "department and agency . . . [to] promptly issue internal directives to implement this section with respect to its foreign intelligence and counterintelligence operations," and directed the Attorney General to "issue guidelines relating to activities of the Federal Bureau of Investigation in the areas of foreign intelligence and counterintelligence."

In 1978, President Carter replaced President Ford's order with his own executive order governing the Intelligence Community, No. 12036. Section 2-2(a) of President Carter's order was more explicit than President Ford's in describing the role of the Attorney General and provided as follows: "The activities described in Sections 2-202 through 2-208 shall be undertaken only as permitted by this Order and by procedures established by the head of the agency concerned and approved by the Attorney General."

The current version of the order, Executive Order 12333, was issued by President Reagan in 1981, and amended by President George W. Bush in 2003, 2004, and most significantly in 2008. (The 2008 amendments are explained here.) The order remains in effect today. It retains the role of the Attorney General in approving Intelligence Community procedures, but also acknowledges the role of the Director of National Intelligence (DNI), a position created by statute in 2004. Under Section 2.3 of Executive Order 12333 (reinforced by Section 3.2), "[e]lements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General . . . after consultation with" the DNI. These AG-approved procedures express many of the key limits on conduct by the U.S. Intelligence Community affecting U.S. persons.

The DOD Manual contains the set of EO 12333 Section 2.3 procedures governing all DOD elements, and the SIGINT Annex is a supplement that is applicable only to activities conducted under the authority of the NSA Director (see EO 12333 § 1.7(c)). Accordingly, and as required by Section 2.3, the SIGINT Annex has been approved by the Attorney General and the Secretary of Defense after consultation with the Director of National Intelligence.

An important regulation of SIGINT is in Procedure 5 of the DOD Manual, which covers "Electronic Surveillance." DOD Manual § 3.5. This part of the DOD Manual begins by requiring Defense Intelligence Components to comply with the Fourth Amendment, and then provides more detailed advice about particular surveillance scenarios. Procedure 5 recognizes that "electronic surveillance targeting a person in the United States" is governed by FISA "except in very limited circumstances." Surveillance targeting a U.S. person abroad must satisfy the FISA Amendments Act and Section 2.5 of Executive Order 12333. For non-U.S. persons abroad, Procedure 5 cross-references FAA § 702. It also addresses emergency situations, surveillance of

a U.S. person abroad in exigent circumstances (such as when the U.S. person has been taken hostage), training and testing surveillance equipment, and technical surveillance countermeasures (TSCM) that are designed to defeat adversaries' surveillance efforts and related measures. With respect to electronic surveillance under executive branch authority, Procedure 5 provides, DIRNSA "will issue appropriate directives and instructions implementing this issuance and the classified annex to govern the conduct of the U.S. SIGINT System." That is the SIGINT Annex.

II. THE SIGINT ANNEX

A. The SIGINT Annex: Summary and Changes from the Prior Annex

The SIGINT Annex reflects a major and long-overdue updating of internal regulations governing signals intelligence. Although the Prior Annex (available beginning on page 118 of this document) is dated 2004, it was last significantly updated in 1988, and it is far behind the technological and legal environment, as well as current operational demands for SIGINT. Part II.B of this paper attempts a very detailed assessment of the new SIGINT Annex, but it may be helpful to begin with an executive summary of the SIGINT Annex and a review of major changes as compared to the Prior Annex. For some readers that will be (more than) enough.

1. SUMMARY OF THE SIGINT ANNEX

The SIGINT Annex is divided into seven sections: (1) General Issuance Information; (2) Collection; (3) Processing and Querying; (4) Retention; (5) Dissemination; (6) Policy, Compliance, Training, and Auditing; and (7) Certain U.S. Person FISA Targets Outside the United States.

The most important aspect of Section 1 is its definition of the scope of the SIGINT Annex. The Annex regulates SIGINT (as opposed to other forms of intelligence); it regulates the entire United States SIGINT System (USSS), including military elements that conduct SIGINT (not just NSA); it covers all relevant SIGINT activity (across all operational phases of the intelligence lifecycle); but it does not cover such activity where it is already regulated by Congress in the Foreign Intelligence Surveillance Act (FISA). The SIGINT Annex does not define "SIGINT" but clearly does not regulate HUMINT and other forms of intelligence activity or direct warfighting. It does not regulate commercial purchases of data.

The exclusion for FISA is very significant because FISA covers a major part of SIGINT targeting U.S. persons or persons in the United States. The SIGINT Annex is fundamentally designed to regulate SIGINT activity that is subject to the Fourth Amendment but not subject to direct statutory regulation. When it enacted FISA in 1978, Congress understood very well that it was leaving some areas of SIGINT to regulation by the executive branch of government, subject to oversight by the Congressional Intelligence Committees.

Section 2 of the SIGINT Annex governs collection. In general, under Section 2.1, SIGINT collection is conducted for one or more of three basic purposes: "to satisfy foreign intelligence or counterintelligence requirements, to provide support to military operations," or in certain circumstances "to protect the safety or enable the recovery of a U.S. person captive." The first two of these purposes make perfect sense, because NSA is both a member of the Intelligence Community and an element of the Department of Defense. The third purpose – rescuing captives – has a venerable pedigree but may be redundant. Other authorized purposes for SIGINT collection – to combat international drug traffickers, transnational organized criminals, and illicit communications under the Communications Act of 1934 – are not mentioned in Section 2.1 but instead are addressed in a separate section (SA § 2.6) on "exceptions" to certain of the normal SIGINT collection rules.

Section 2.2 of the Annex sets out general requirements for SIGINT collection. First, the USSS may not "intentionally target U.S. persons or persons in the United States unless authorization has been obtained in accordance with this section or FISA." Given the reach of FISA, as noted above, this is a significant limit. Second, with respect to U.S. persons or persons in the United States, the USSS must "limit SIGINT collection" to "collect no more information than is reasonably necessary" and perhaps also to use the least intrusive means feasible. Third, the USSS must conduct targeted collection (as opposed to bulk collection) "whenever practicable," normally by using selection terms or other discriminants; PPD-28 continues to restrict bulk SIGINT collection to six defined categories. Fourth, the USSS must take "reasonable steps" to determine the nationality and location of targets (to inform application of the appropriate rules, which often depend on nationality and location). Fifth and finally, the USSS must try to reduce the amount of incidental collection of domestic communications or communications concerning U.S. persons.

Section 2.3 of the Annex prescribes several factors that the USSS must "consider" both in conducting collection and in developing collection techniques. These factors include methods to limit collection of non-pertinent information that identifies a U.S. person (USPI); methods to limit collection of other non-pertinent information; methods of filtering non-pertinent information earlier rather than later without compromising mission; whether collection qualifies for enhanced ("special circumstances") regulation under the DOD Manual; and whether "additional approvals or civil liberties and privacy protections are needed."

Section 2.4 imposes two "prohibitions" on SIGINT. There is a rule against "reverse targeting," in which the person or entity from or about whom the government is seeking information is not the identified (nominal) target of the collection. There is also a general rule against intentional collection of domestic communications, subject to three exceptions: as authorized by FISA; as authorized by certain provisions of the DOD Manual governing training, testing and countermeasures; and as authorized by Section 2.5 of the SIGINT Annex itself, which is discussed next.

Section 2.5 of the SIGINT Annex, which deals with "Limitations" on SIGINT collection, is the longest and most complex provision in the Annex, spanning more than five pages. It

addresses (a) limitations on certain collection methods; (b) limitations on collection targeting U.S. persons; (c) special rules concerning U.S. person captives abroad; and (d) limitations on collection targeting non-U.S. persons in the United States.

Section 2.5.a. limits SIGINT collection using selection terms (which, as noted above in the discussion of Section 2.2, is required whenever practicable). Where selection terms "are reasonably likely to result in, or have resulted in, collection of" communications concerning U.S. persons – even if not designed to do so – the USSS must undertake certain (redacted) efforts that are designed to reduce or defeat collection of such communications (and data related to those communications) that are not pertinent to an authorized collection purpose. Two specific (and redacted) examples are described. First, when conducting SIGINT over radio channels that have a terminal in the United States, the USSS must "target non-U.S. persons outside the United States," and must also use selection terms unless the channel in question is used "exclusively by a foreign power." Second, a more heavily redacted scenario involves something "Used by a Foreign Entity" that has "a terminal in the United States that service a U.S. person." Unlike the first scenario, this second collection scenario is not described as being limited to radio communications, and so it may apply to the acquisition of wire communications or other things. This second collection scenario requires a certification from DIRNSA or his delegee to the Attorney General confirming that the collection target is a non-U.S. person located abroad, that the collection is not governed by FISA, and that it has a foreign intelligence or counterintelligence purpose.

Section 2.5.a. also limits the use of SIGINT "surveys," which are reviews of "the signals environment" to identify "signals or communications" that are important for future collection. In keeping with historical practice, surveys may be conducted to find signals or communications of intelligence value, to find signals or communications of value in developing cryptanalytic capabilities, to rule out unwanted signals, or to reveal U.S. communications vulnerabilities. A survey must be limited in scope and duration and may not be used as a substitute for authorized collection.

Section 2.5.b. imposes limits on collection targeting U.S. persons. Regardless of where the U.S. person is located, such collection is permitted only if it is not governed by FISA and if one of three enumerated circumstances exists: consent; exigent circumstances; or where the Attorney General determines that the U.S. person is an agent, officer or employee of a foreign power and the purpose of the collection is to acquire significant foreign intelligence or counterintelligence. This last circumstance is similar to the standard set by FAA § 704, 50 U.S.C. § 1881c.

Section 2.5.c applies to SIGINT collection concerning U.S. persons abroad who have been taken captive by a non-U.S. person. This is one of the three authorized purposes for SIGINT collection specified in Section 2.1 as discussed above. It involves SIGINT collection as necessary to protect the safety or enable the recovery of the U.S. person, including limited SIGINT targeting the U.S. person (e.g., directed against his mobile phone) for up to 90 days at a time. Section 2.5.c. does not confer authority to target any U.S. person except the captive or

any non-U.S. person in the United States. This exception has intuitive appeal and a venerable pedigree, but its legal rationale is not entirely clear. Depending on the facts of the particular collection, it may rest on a theory of exigent circumstances (and as such may function as a subset of more general authority to collect SIGINT in exigent circumstances) or implied consent; or it may reflect other legal theories.

Section 2.5.d. limits collection targeting non-U.S. persons in the United States. Here, as under Section 2.5.b., the baseline requirement is that the collection not be regulated by FISA; in addition, at least one of several enumerated circumstances must apply. Those circumstances include consent; two redacted circumstances; where the Attorney General finds probable cause that the person is an agent of a foreign power and there is a purpose to acquire significant foreign intelligence or counterintelligence; and for 72 hours in the case of a FAA § 702 (50 U.S.C. § 1881a) roamer (cf. 50 U.S.C. § 1805(e)).

Section 2.6 of the SIGINT Annex identifies two exceptions to certain of the requirements in Section 2. First, notwithstanding the limits in Sections 2.5.a. (concerning surveys) and 2.5.b. (limiting targeting of U.S. persons), the USSS may target "U.S. persons outside the United States who are suspected of involvement in international narcotics trafficking or transnational organized crime." This is consistent with Section 2.6 of Executive Order 12333 and 50 U.S.C. § 3039(a), and it has roots in Appendix A to the Prior Annex and Annex J to USSID-18. Collection under this exception is permitted "only … where the communicants do not have a reasonable expectation of privacy in [the collected] radio communications and the communications are not otherwise protected by the Fourth Amendment." SA § 2.6.a. Second, notwithstanding the prohibition on collecting domestic communications in SA § 2.4.a, and the limitations on collection in SA § 2.5, the USSS may collect "illicit communications" under the Communications Act of 1934 in certain circumstances with the approval of the Attorney General. Annex F to USSID-18 explains that "'illicit communications' means a communication transmitted in violation of either the Communications Act of 1934 and regulations issued thereunder or international agreements, which because of its explicit content, message characteristics, or method of transmission, is reasonably believed to be a communication to or from an agent or agents of foreign powers, whether or not U.S. persons."

Section 3 of the SIGINT Annex governs processing and querying of collected information. Under Section 3.2, the USSS "may process [raw] SIGINT to prepare data for analysis." Examples of permitted processing include "[p]rocessing information to characterize or understand signals and communications," taking steps to "convert information to an intelligible form intended for human inspection," reverse engineering malware, and tagging data. Under Section 3.2.a.(4), processing may include "[c]ombining SIGINT information with other information to facilitate activities such as data correlation, retrieval, formatting, and conversion" – e.g., to make it more suitable for querying – but under Section 3.2.a.(6) it also includes "[p]rocessing information to limit USPI and non-pertinent information" in keeping with the "considerations" set out in Section 2.3. The use of discriminants in processing that occurs promptly after acquiring large data sets may save the acquisition of those data sets from being considered "bulk collection" under Section 2, footnote 5 of PPD-28. The SIGINT Annex, however, uses the DOD Manual's

definition of "collection," which does not seem to exempt information discarded after prompt post-acquisition processing unless the processing is "momentary," as in the case of something like a packet-sniffer. See SA § G.2; DOD Manual § G.2. In any event, under the Annex, if "the contents of communications are retrieved for human inspection" during processing, the querying rules apply. SA § 3.2.b.

Sections 3.3 and 3.4 govern querying. Queries may be conducted for the same three purposes as collection under Section 2.1, as discussed above. Although the SIGINT Annex does not define the term "query," the basic meaning is an inquiry designed to retrieve information from storage. Queries "using selection terms that are reasonably likely to result in, or have resulted in, the retrieval of communications to, from, or about a U.S. person" must be "designed" so that they "defeat, to the extent practicable under the circumstances, the retrieval of those communications, or data related to such communications, not relevant to" an authorized purpose. As noted above, a similar rule applies to collection with selection terms under Section 2.5.a.

Under Section 3.4, queries that are affirmatively designed to retrieve communications concerning a U.S. person or a person in the U.S. are permitted only in certain circumstances. Those circumstances include consent; where the subject of the query is a current FISA target; two redacted circumstances (one of which involves cyber threat activity); for 72 hours in the case of a FAA § 702 roamer; with the approval of DIRNSA in certain defined circumstances; and with the approval of the Attorney General in certain other circumstances. Taken together, these authorized circumstances permit U.S. person queries in a way that is more precisely defined (more prescriptive), and broader, than what was permitted under the Prior Annex, which treated queries principally as collection events and focused on standards requiring the U.S. person to be an agent of a foreign power. The SIGINT Annex therefore moves some of the way, but not all of the way, towards permitting querying for any legitimate foreign intelligence or related purpose. It may reflect a view that the Fourth Amendment permits more in the way of queries of previously collected data than it does for collection itself, even when the data were not collected under statutory requirements or with judicial approval. In any event, as a statutory matter, collection targeting U.S. persons, including U.S. persons abroad, is constrained by traditional FISA, FAA § 704, and Section 2.5 of Executive Order 12333. In some cases, querying may result in dissemination of a subset of foreign intelligence data that could and perhaps would previously have been disseminated in its entirety.

Finally, Section 3.5 of the SIGINT Annex provides that the limitations on queries discussed above do not apply to authorized "communications metadata analysis, including contact chaining." In such cases, metadata analysis and contact chaining may proceed "without regard to the physical location or nationality of any of the communicants or the location or registration of any device." This exception carries forward a version of the 2008 Special Procedures Governing Communications Metadata Analysis (SPCMA) that were adopted as a supplement to the Prior Annex.

Section 4 of the SIGINT Annex governs retention of information not subject to FISA, modifies certain retention periods in the DOD Manual, and implements 50 U.S.C. § 1813. Section 4.2 of the Annex sets a general 5-year retention period for unevaluated (raw) SIGINT; enciphered data can be retained for as long as needed to permit exploitation and for five years thereafter. Section 4.3 allows DIRNSA to authorize an additional retention period of up to 20 years for unevaluated SIGINT if he submits an explanatory certification to the Congressional Intelligence Committees. Section 4.4 sets retention periods for evaluated SIGINT. For non-domestic communications that do not contain USPI, retention may be permanent if the information is (or is necessary to understand) foreign intelligence or counterintelligence. For non-domestic communications that do contain USPI, permanent retention is authorized under the same standard. Communications that contain USPI may also be retained, with masking if appropriate, for cryptanalysis and related purposes. With notice to the Congressional Intelligence Committees, communications necessary to protect against an imminent threat to human life may be retained in excess of five years. Extended retention is also permitted for technical assurance or compliance purposes with reporting to Congress and DOD. Section 4.5 of the SIGINT Annex includes an exception for communications metadata, including the results of contact chaining and other analysis of metadata, that is analogous to the exception for metadata analysis in Section 3.5.

Under Section 4.6.a. of the SIGINT Annex, the USSS generally may not retain domestic communications in which a person has a reasonable expectation of privacy and a warrant would be required to collect the communications for law enforcement purposes. The only exception is if the Attorney General determines that retention is lawful and the contents indicate a threat of death or serious bodily harm. Under Section 4.6.b., communications acquired by inadvertent targeting of a non-consenting U.S. person generally must be destroyed upon recognition. The only exception applies where DIRNSA or a delegee determines that FISA does not preclude retention; that retention accords with Sections 4.2-4.5; and the communications contain evidence of a crime, significant foreign intelligence or counterintelligence, or information indicating a threat of serious harm to life or property. Section 4.6.c. imposes a similar destruction requirement for communications acquired as a result of inadvertent targeting of certain non-consenting non-U.S. persons in the United States. Redactions make it difficult to know exactly who and what is protected by this provision.

Section 5 of the SIGINT Annex governs dissemination of information, the final stage of the intelligence lifecycle. The dissemination rules in the SIGINT Annex are generally consistent with similar rules in minimization procedures under FISA. Under Section 5.2, USPI may not be included in a SIGINT dissemination unless the recipient has a legitimate need for the USPI and one of several conditions exists: (a) consent; (b) the USPI is publicly available; (c) the USPI is needed to understand or assess the intelligence; (d) the USPI is evidence of a crime that is being disseminated for law enforcement purposes; (e) the USPI is disseminated to protect the safety or enable the recovery of a U.S. person captive held abroad by non-U.S. persons; or (f) the dissemination is otherwise required by law or directive. Section 5.3 governs dissemination of information obtained from a survey (see discussion of SA § 2.5.a. above). In keeping with the basic purpose of a survey, information “necessary for cataloging the constituent elements of

the signals environment may be disseminated to the extent that such information is not USPI." In keeping with similar rules under FISA, the Annex provides that "[c]ommunications equipment nomenclature" – e.g., the brand of a router or switch – is not treated as USPI even if the brand name is of an American company.

Section 6 of the SIGINT Annex addresses policy, compliance, training, and auditing. This includes various measures "to ensure compliance with the requirements of this annex" and the DOD Manual. Under Section 6.2, DIRNSA must issue policies to implement the SIGINT Annex in coordination with legal, civil liberties, and privacy officials. Section 6.5 requires auditing and appropriate internal controls for collection, access, queries, retention, and dissemination. Under Section 6.6 of the Annex, NSA must make certain reports to the Department of Justice and/or other entities.

Section 7 of the SIGINT Annex implements FAA § 704, 50 U.S.C. § 1881c, which regulates intelligence collection targeting U.S. persons abroad. Prior to enactment of the FAA in 2008, such collection was governed principally by Section 2.5 of Executive Order 12333. Section 7 of the SIGINT Annex establishes rules under which the USSS can comply with the FAA. It includes a sensible express prohibition on reverse targeting.

2. CHANGES FROM THE PRIOR ANNEX

The new SIGINT Annex seems to reflect at least three significant changes as compared to its predecessor, almost all of them apparently designed with operational personnel and the current SIGINT environment in mind.

First, the new SIGINT Annex is generally more prescriptive than its predecessor. It makes certain requirements and authorizations explicit where they previously were implicit. That is, the Annex tries to connect the dots among its own elements, explaining how certain provisions interact to permit or restrict certain operational possibilities that regularly arise. Effectively, the new SIGINT Annex has a series of FAQs built into the body of the document. In the same vein, the new SIGINT Annex tries to consolidate guidance, bringing requirements within its own four corners to simplify research into the governing rules. This effort is manifest in the document's length: where the Prior Annex consisted of around a dozen substantive pages, the new SIGINT Annex has around 35 such pages.

The most important example of expanded prescription probably concerns querying. The Prior Annex did not separately regulate querying of data with U.S. person identifiers. Instead, it effectively treated such queries as targeting or collection decisions. See Prior Annex § 4.A.1 at pages A-5 to A-7; see also Prior Annex § 4.A.3.(a) at pages A-8 to A-9. The current Annex, however, deals explicitly and in greater detail with querying in Sections 3.3 and 3.4. As discussed in Part II.B.3 below, this probably reflects growing national attention to querying, including as an activity that is separate from collection, as reflected in provisions added to the FISA Amendments Act in 2018. 50 U.S.C. § 1881a(f). The SIGINT Annex also reflects a general shift from the Prior Annex, moving away from U.S. person querying standards that emphasized

status as an agent of a foreign power, and towards (but not all the way to) standards that emphasize a legitimate foreign intelligence or related purpose for the query. Other examples of greater prescription include an express prohibition on reverse targeting (SA § 2.4.b), an express cat's paw provision (SA § 1.3.b) that corresponds to Section 2.12 of Executive Order 12333, and more developed limits on surveys (SA § 2.5.a.2).

One counterexample concerns individual consent to SIGINT. The Prior Annex included a specific form containing the precise words to be used to obtain consent for SIGINT collection (e.g., against a member of the IC). See Prior Annex at page A-14. The new SIGINT Annex does not include such a form, but merely requires valid consent without prescribing specific words to obtain that consent. Annex H to USSID-18 contains model consent forms, and the new version of USSID-18, or other guidance to be issued under the authority of SA § 6.2, may do so. But the SIGINT Annex itself is written at a higher level of generality (this shift may also affect the extent to which deviations or violations must be reported to external overseers, whether in DOD or elsewhere). In this area, therefore, the SIGINT Annex is less prescriptive than its predecessor.

A second important change from the Prior Annex is related to the first change: the new SIGINT Annex takes account of statutorily required expansions of NSA's compliance and civil liberties infrastructure. Under 50 U.S.C. § 3602(b), as of 2010, "[t]here is a Director of Compliance of the National Security Agency, who shall be appointed by the Director of the National Security Agency and who shall be responsible for the programs of compliance over mission activities of the National Security Agency." The Director of Compliance is the only NSA officer other than DIRNSA who is specified in the National Security Agency Act (50 U.S.C. §§ 3601-18), which generally provides for secrecy as to "names, titles, salaries, or number of the persons employed by such agency." 50 U.S.C. § 3605(a). In addition, NSA's Director of the Civil Liberties and Privacy Office, required by 2018 amendments to 42 U.S.C. § 2000ee-1, is responsible for advising NSA on protection of privacy and civil liberties. NSA today has a much more developed set of personnel and procedures for dealing with compliance, privacy and civil liberties than it did when the Prior Annex was in effect. This also explains Section 6 of the new Annex, which applies to "Policy, Compliance, Training, and Auditing." Outside of the USSS, the Privacy and Civil Liberties Oversight Board (PCLOB) has had a significant impact on SIGINT, issuing recommendations for privacy and civil liberties officers in the executive branch, as well as a series of reports on the USA Freedom Act, PPD-28, FAA § 702, and FISA's business records provisions. Section 3 of the Prior Annex (page A-4), which authorized DIRNSA or a designee to "issue appropriate directives and instructions implementing these procedures," is much less extensive than Section 6 of the SIGINT Annex, and existed in a much less developed environment for privacy and civil liberties.

In general, NSA's expanded compliance and civil liberties infrastructure may correspond to increased prescription in the SIGINT Annex. There are more professionals at the agency now charged with testing and overseeing the regulation of SIGINT (and there is also a National Security Division at the Department of Justice that is dedicated in part to intelligence oversight, although the DOJ Office of Intelligence Policy and Review (OIPR) also conducted intelligence oversight before NSD was established in 2006). It therefore should not be surprising to see

more precision and prescription in the Annex. The reduced prescription with respect to the precise words needed to obtain consent may reflect a sense that these professionals, and the lawyers at NSA, can adequately assess the validity of consent under the Supreme Court's "totality of the circumstances" test without the use of a rigid formula. See, e.g., *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973). It is worth noting that, in recent years, while NSA certainly has had its share of compliance problems, the agency has also more or less voluntarily receded from certain lawful collection, including certain upstream collection, bulk Internet metadata collection, and (effectively) renewal of the USA Freedom Act call detail records program.

Third, the SIGINT Annex appears to be more technology neutral than the Prior Annex. For example, the Prior Annex had special rules for voice and fax communications that are not present in the SIGINT Annex. See Prior Annex § 4.A.1.(f) at page A-7. Where the Prior Annex often distinguished rules by the type of signal being collected – e.g., treating radio frequency (RF) differently than wired communications – the new SIGINT Annex seems to emphasize phases of the SIGINT lifecycle, such as collection, processing, and querying. This difference can be overstated: even the new SIGINT Annex refers specifically to RF collection in certain areas, see SA § 2.5.(a)(1)(A), and the Prior Annex did refer separately to collection, processing, retention, and dissemination, see pages A-5 to A-11. But the emphasis has shifted, in part because the SIGINT environment itself has shifted in ways that makes it less useful for operators to focus too much on signal type, with more complex, diverse, and hybrid communications networks and systems increasingly the norm. This change also overlaps to some degree with the first change noted above: the SIGINT Annex provides guidance that is designed for operators and tailored based on a recognition that the privacy and related risks in each phase of the SIGINT lifecycle may be different.

Apart from these three structural changes – more prescription, more reliance on NSA's compliance and civil liberties infrastructure, and more technology neutrality – there is the question of how the Annex strikes the balance between privacy and security. For some readers, the only important question may be whether the SIGINT Annex gives the government more or less authority than it previously enjoyed.

The question is important, but for at least three reasons it is very difficult to answer authoritatively. First, the unclassified documents do not reveal all of the relevant rules, regulations, procedures and practices. The Prior Annex and the new SIGINT Annex both have redactions, as do more detailed guidance documents such as USSID-18. Moreover, some relevant written materials are not available or do not yet exist (e.g., anticipated revisions to USSID-18). The IC's transparency with respect to SIGINT has increased dramatically in recent years, but much of its work remains classified, overseen by the Congressional Intelligence Committees and various others, but not fully visible to our adversaries or to the American public. This is not meant to denigrate the importance of largely unclassified materials such as the SIGINT Annex; it is only to recognize that, by necessity, they do not tell the entire story of SIGINT.

Second, the legal and technological environments in which SIGINT is conducted have both changed dramatically since the Prior Annex was adopted. The FISA Amendments Act of 2008, for example, increased the government's authority to target non-U.S. persons reasonably believed to be abroad in 50 U.S.C. § 1881a, but restricted its authority to target U.S. persons reasonably believed to be abroad in 50 U.S.C. § 1881c. Judicial interpretations of the Fourth Amendment have likewise evolved significantly in recent years, in decisions ranging from *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), to *Carpenter v. United States*, 138 S. Ct. 2206 (2018). As for technology: in 1988, when the Prior Annex was last significantly revised, the Internet was not yet part of daily life. Some elements of the U.S. government claim that they are "going dark" as a result of technological changes, while civil libertarians and others claim that technology has created a "golden age of surveillance." My own view is that digital network technology has reduced both privacy and security, but in any event there is no doubt that technology has had a major impact on SIGINT. Constitutional, statutory, and technological changes complicate any effort to compare relative SIGINT authority in 1988 and today.

Third, and perhaps most importantly, the Prior Annex and the SIGINT Annex regulate a very wide and dynamic range of activity. Both documents are immensely complex and the differences between them do not all point in one direction. Looking at any one change in a vacuum can be misleading. For example, as noted above, we know that NSA in recent years has receded from certain lawful collection, but it is hard to assess the net significance of these choices without knowing whether and how other forms of collection may have expanded.

A simple answer to the question therefore risks reductionism. To avoid that, Part II.B takes up a detailed review of the SIGINT Annex, noting differences from the Prior Annex where applicable.

B. The SIGINT Annex: Detailed Review

The SIGINT Annex is divided into seven sections: (1) General Issuance Information; (2) Collection; (3) Processing and Querying; (4) Retention; (5) Dissemination; (6) Policy, Compliance, Training, and Auditing; and (7) Certain U.S. Person FISA Targets Outside the United States. This structure will be quite familiar to students of SIGINT and other forms of electronic surveillance: putting aside the prefatory material in Section 1 and the general policy material in Section 6, the remaining sections of the Annex address the usual minimization categories – acquisition, retention, and dissemination – with two additional sections (on querying and on surveillance of U.S. Persons abroad) that have well-understood counterparts in the FISA Amendments Act of 2008. Each of the seven sections is reviewed below.

1. GENERAL INFORMATION

Section 1 of the SIGINT Annex includes a recitation of SIGINT authority in Executive Order 12333 and the DOD Manual (§ 1.1); a statement on the applicability of the Annex (§ 1.2); and a set of general provisions (§ 1.3). The SIGINT Annex explicitly regulates the entire United States SIGINT System (USSS), SA § 1.2.a, which is defined as the "organization unified under" the Director of NSA's (DIRNSA's) "authority to conduct SIGINT." SA § G.2. See, e.g., Executive Order 12333 § 1.7. The USSS therefore includes "NSA and components of the Military Services (including the U.S. Coast Guard) that are authorized to conduct SIGINT activities." SA § G.2. Although foreign cryptologic partners (e.g., NSA second- and third-party partners) are not themselves part of the USSS, SA § G.2, the Annex applies to the USSS's work with foreign partners, in accord with Section 2.12 of Executive Order 12333. SA § 1.3.b. As NSA's SIGINT FAQ website explains, "NSA is prohibited from requesting any person to undertake activities that NSA itself is prohibited from conducting."

Section 1 includes a mechanism for delegations, interpretations, exceptions, and amendments of the Annex via NSA's Office of General Counsel (§ 1.3.d); a reference to special rules for attorney-client privileged communications (§ 1.3.e.); and a limited exception for due diligence activities in aid of adherence to its requirements, which appear to be concerned chiefly with determining "foreignness" – e.g., that a collection target is a non-U.S. person and/or located abroad (§ 1.3.f). This can be important for collection avoidance as much as for affirmative collection, and Section 1.3.f.(1)(a) provides that "due diligence activities" directed at determining foreignness "will be designed to limit to the greatest extent practicable the review of the contents of communications that contain USPI," a sensible requirement that appears not to exist in any other IC guidelines issued under Section 2.3 of Executive Order 12333.

There is also an explicit authorization (SA § 1.3.f.(4)) to "process, query, retain, and disseminate information to comply with a litigation hold, preservation directive, or court order," among other things. In the past, the government has had difficulty with confusion in this latter area, including a conflict between a directive to delete data (from the FISA Court imposing minimization requirements) and a directive to retain the data (from a different federal court in the context of civil litigation). See, e.g., *In re Application of FBI for an Order Requiring the Production of Tangible Things*, No. BR 14-01 (Mar. 21, 2014). Section 1.4 of the SIGINT Annex is apparently designed to be consistent with DOD Manual 8910.01 governing information collections. The Annex also contains a standard statement that it is internal guidance that does not create any individual rights (§ 1.3.c), in accord with *United States v. Caceres*, 440 U.S. 741 (1979).

Two aspects of Section 1 are worth emphasizing and are discussed in more detail below: (a) the scope of the Annex, meaning the areas and types of SIGINT activity that it does and does not purport to regulate; and (b) the rules that it uses for determining whether or not a person is a U.S. person.

a. *Scope*. The most important threshold question answered in Section 1 concerns the subject-matter scope of the SIGINT Annex. The Annex defines its scope in three ways: it covers SIGINT (as opposed to other forms of intelligence); it covers all relevant SIGINT activity (across all operational phases of the intelligence lifecycle); but it does not cover such activity where it is already regulated by Congress in FISA. This is a conventional and appropriate way of stating generally what falls under the SIGINT elements of Executive Order 12333 and its subordinate procedures, but it is much easier to state generally than to describe specifically. It will be helpful to survey the covered landscape, and its perimeter, in more detail.

At the outset, in its title and in Sections 1.1-1.2, the Annex explains that it regulates SIGINT (signals intelligence), which includes COMINT (communications intelligence), ELINT (electronic intelligence), FISINT (foreign instrumentation intelligence) and related information like telemetry, radar emissions, and direction-finding data. SA § 1.2.a. NSA elsewhere describes SIGINT as "intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems," which is consistent with traditional understandings of SIGINT. See, e.g., Army FM 2-0 Chapter 8. In its report on PPD-28, the Privacy and Civil Liberties Oversight Board (PCLOB) criticized the government for adopting SIGINT regulations without precisely defining the term. See, e.g., Report at 12, 24. The SIGINT Annex does not provide much more detail, bringing to mind the old joke that "SIGINT" is whatever NSA (or the USSS) does when it is operating under DIRNSA's SIGINT authorities. The Annex effectively approaches the question from the other direction, regulating the entire USSS but excluding from regulation the "non-SIGINT activities" of the relevant organizations. SA § G.2 (definition of "USSS"). Under EO 12333 § 1.7(c)(2), as NSA will remind anyone who is willing to listen, "[n]o other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director" of NSA.

In any event, it is clear that the Annex eschews regulation of non-intelligence activities – e.g., direct warfighting – as well as other forms of intelligence, such as GEOINT, HUMINT, IMINT, MASINT and OSINT. Of course, the major INT disciplines are not the only way to sub-divide intelligence – for example, the 2019 National Intelligence Strategy separately describes strategic, anticipatory, current operations, cyber threat, counterterrorism, counterproliferation, and counterintelligence and security intelligence. But the six major INT disciplines are meaningful from the perspective of collectors and other operational personnel who generate intelligence, as opposed to policymakers who consume it, and so the SIGINT Annex, as a document that regulates operational personnel, is appropriately focused.

With respect to SIGINT, the Annex covers "collection, processing, querying, retention, and dissemination" of COMINT, as well as ELINT, FISINT, and related (e.g., telemetry) activities "that implicate the Fourth Amendment." SA § 1.2.a. It also covers (SA § 1.2.a) collection of "any … non-communications and non-communications related data … conducted by the USSS that implicate[s] the Fourth Amendment." This embraces all of the relevant phases of the intelligence lifecycle (excluding planning), from initial acquisition to finished reporting, and corresponds to the breadth required by the Annex's ultimate parent authority, Section 2.3 of

Executive Order 12333, which provides that "[e]lements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with [properly approved] procedures" (emphasis added). The wide embrace of the EO and the Annex is also appropriate because the FISA Court (and other courts) have indicated that post-acquisition activities and later treatment of data may bear on the constitutionality of front-end intelligence collection. See NSIP § 17:11 at 717. Cf. Prior Annex § 1 (page A-1) ("These procedures … govern the conduct by [USSS] of [SIGINT] activities that involve the collection, retention, and dissemination of communications originated or intended for receipt in the United States, and [SIGINT] activities that are directed intentionally against the communications of a United States person who is outside the United States. … They do not apply to [SIGINT] activities that are not required under Executive Order 12333 to be conducted pursuant to procedures approved by the Attorney General" (emphasis in original)).

By its terms, however, the Annex does not apply to SIGINT activities "conducted pursuant to FISA," apart from "collection activities that target U.S. persons outside the United States under Section 2.5 of E.O. 12333 and Sections 704, 705(b), or 705(c)" of the statute, 50 U.S.C. §§ 1881c-1881d. SA § 1.2.b. It is worth exploring both why the FISA-based exclusions make sense, and precisely what they mean for the scope of the SIGINT Annex.

The FISA-based exclusions from the SIGINT Annex make sense because FISA itself, and the many and varied procedures that must be adopted pursuant to FISA, already regulate who may be targeted and the acquisition, retention and dissemination of information (FAA § 702 also explicitly regulates the querying of information) under the supervision of the FISA Court. See 50 U.S.C. §§ 1801(h), 1821(4), 1881a(e)-(f), 1881b(b)(1)(D). Where FISA applies, therefore, Congress and the FISA Court have already set standards, and the SIGINT Annex has no major gap to fill.

It is, however, both sensible and necessary for the SIGINT Annex to regulate FAA § 704 collection because Section 704 requires FISA Court approval only of dissemination procedures, not acquisition or retention procedures. See 50 U.S.C. § 1881c(c)(1)(C). Overall, Section 704 has much lighter requirements than traditional FISA. For example, a Section 704 application need not describe the nature of the information sought, the type of communications or activities to be subjected to acquisition, or the means by which the acquisition will be conducted and whether physical entry is required to effect it. Indeed, the FISA Court lacks jurisdiction even to "review the means by which an acquisition . . . may be conducted" under FAA § 704. 50 U.S.C. §§ 1881c(c)(3)(A), 1881c(c)(5). Accordingly, an order under Section 704 has no significant specifications – it does not identify the facilities or places at which collection will be directed, the nature of the information being sought, the type of communications or activities to be subjected to acquisition, or the means of effecting the acquisition. Were it to rely solely on FAA § 704 for regulation of SIGINT activity under that law, therefore, the Annex would leave significant gaps when measured against the requirements of Section 2.3 of Executive Order 12333 (and perhaps also the Fourth Amendment).

Put differently, Congress intended in FISA to regulate SIGINT activity all the way from acquisition to dissemination under traditional FISA and FAA § 702, but effectively left it to the executive branch to self-regulate, subject to oversight from the Intelligence Committees, in other areas including acquisition and retention (but not dissemination) under FAA § 704. This was a very deliberate decision: when it enacted FISA in 1978, Congress understood that the statute did not "bring the overseas activities of the U.S. intelligence community within its purview," but noted "with approval that electronic surveillance of American citizens while abroad has been limited in part both by the President's Executive Order applicable to the U.S. intelligence community and by procedures approved by the Attorney General." H.R. Rep. No. 95-1283 (1978), 95th Cong. 2d Sess. 51 & n.26 (1978) (hereinafter HPSCI 1978 FISA Report). The SIGINT Annex regulates mainly in the spaces left open by Congress.

The FISA exclusions significantly limit the scope of the SIGINT Annex, but the extent of the limit, which depends on the regulatory reach of FISA, is not always easy to discern. As described in greater detail in NSIP Chapters 7 and 16, traditional FISA's four-part definition of "electronic surveillance" in 50 U.S.C. § 1801(f), and its definition of "physical search" in 50 U.S.C. § 1821(5), determine the statute's reach. Where NSA engages in SIGINT activity that meets these definitions, it is required to use traditional FISA. See 50 U.S.C. §§ 1809, 1812, 1827; NSIP Chapters 7, 15. The Annex does not dispute this. To understand the Annex, therefore, it is necessary to understand what is, and what is not, "electronic surveillance" or a "physical search" as defined by FISA. The former definition has four sub-parts.

First, it is "electronic surveillance" under FISA to acquire via surveillance device "any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f)(1). As the House Intelligence Committee explained when it enacted the statute in 1978:

> Paragraph (1) protects U.S. persons who are located in the United States from being targeted in their domestic or *international* communications without a court order no matter where the surveillance is being carried out. The paragraph covers the acquisition of the contents of a wire or radio communication of a U.S. person by intentionally targeting, that particular, known U.S. person, provided that the person is located within the United States. Thus, for example, any watchlisting activities of the National Security Agency conducted in the future, directed against the international communications of particular U.S. persons who are in the United States, would require a court order under this provision.

HPSCI 1978 FISA Report at 50. Under FISA, as under the SIGINT Annex, the "target" of collection is the person or entity from or about whom information is deliberately sought by the government. See *In re Sealed Case*, 310 F.3d 717, 740 (FISCR 2002) (citing HPSCI 1978 FISA Report at 73)); SA § G.2.

Second, it is also "electronic surveillance" under FISA to acquire with a surveillance device "any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States" (other than computer trespassers under 18 U.S.C. § 2511(2)(i)). 50 U.S.C. § 1801(f)(2). This provision applies whether or not the surveillance has a particular target. As the legislative history explains, "one party to the wire communication may be outside the United States if the acquisition occurs within the United States. Thus, either a wholly domestic telephone call or an international telephone call can be the subject of electronic surveillance under this subdefinition if the acquisition of the content of the call takes place in this country." HPSCI 1978 FISA Report at 51.

Third, it is "electronic surveillance" intentionally to acquire via surveillance device "any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States." 50 U.S.C. § 1801(f)(3). As the 1978 HPSCI report explains, "[t]his part of the definition would reach not only the acquisitions of communications made wholly by radio but also the acquisition of communications which are carried in part by wire and in part by radio, where the radio transmitted portion of those communications are intercepted." HPSCI 1978 FISA Report at 52. That is because FISA (unlike the federal Wiretap Act, 18 U.S.C. § 2510(1)) defines a "wire communication" as a communication only "while it is being carried by a wire," 50 U.S.C. § 1801(*l*), leaving room for the same communication to be a "radio communication" while it is being carried by radio wave.

The legislative history also notes an important distinction between the second and third subsections of the definition: "The territorial limits of this [third] subdefinition are not dependent on the point of acquisition, as is the case with subdefinition (2), but on the locations of the sender and intended recipients of the communication. Thus, the acquisition of radio communications outside the territorial limits of the United States would be covered if all of the parties were located within the United States. Only acquisition of those domestic radio communications made with a reasonable expectation of privacy where a warrant would be required for law enforcement purposes would be included in the term 'electronic surveillance.' This would exclude for example, commercial broadcasts, as well as ham radio and citizen band radio broadcasts." HPSCI 1978 FISA Report at 52.

Fourth, it is "electronic surveillance" to install or use a surveillance device "in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f)(2). This provision applies to data in electronic storage, such as e-mail, and to surveillance via hidden microphones. The 1978 legislative history explains: "This is intended to include the acquisition of oral communications made by a person exhibiting an expectation that such utterances are not subject to acquisition, under circumstances justifying such expectation. In addition, it is meant to include the installation of 'beepers' and 'transponders,' if a warrant would be required in the ordinary criminal context … It could also include miniaturized television cameras and other sophisticated devices not aimed merely at communications." HPSCI 1978 FISA Report at 52.

Taken together, the four parts of FISA's definition of "electronic surveillance" cover a lot of ground: as Procedure 5 of the DOD Manual recognizes, "electronic surveillance targeting a person in the United States" is governed by FISA "except in very limited circumstances."

In addition, it is generally a "physical search" under FISA to conduct "any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes," 50 U.S.C. § 1821(5). This would include surveillance using a thermal imager or other non-standard device of the sort addressed by the Supreme Court in *Kyllo v. United States*, 533 U.S. 27 (2001).

These traditional FISA definitions, however, intentionally omit "acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in" FISA. 18 U.S.C. § 2511(2)(f); 50 U.S.C. § 1821(5).

In particular, at least to first order of approximation, there are four major SIGINT collection scenarios that are outside the scope of traditional FISA (see NSIP § 7:17):

(1) where all parties to an acquired wire or radio communication are located abroad;

(2) where the target is located abroad and the surveillance (acquisition) occurs abroad;

(3) where the target is a non-U.S. person (or there is no specific target) and the surveillance (acquisition) occurs abroad; and

(4) where at least one intended party to an acquired radio communication is located abroad and the target is a non-U.S. person (or there is no specific target).

Section 702 of the FAA, 50 U.S.C. § 1881a, as a part of FISA, is also out of scope for the SIGINT Annex. See SA § 1.2.b. Section 702 covers collection targeting non-USPs reasonably believed to be abroad, see 50 U.S.C. §§ 1881a(a) & (b)(3), involving assistance from an electronic communications service provider (ECSP), see 50 U.S.C. § 1881a(h)(2)(A)(vi), regardless of whether the collection would be "electronic surveillance" or a "physical search" under traditional FISA (and, perhaps, even if it would be neither, see NSIP § 17:8 text & nn.32-34). Unlike traditional FISA, however, FAA § 702 does not purport to exert any preclusive effect or assert exclusivity of regulation with respect to the targeting of non-U.S. persons reasonably believed to be located abroad. That is, Section 702 is an optional statutory regime that NSA may, but need not, use to target such persons (e.g., if it wants to compel assistance from an

ECSP). If the government elects to proceed under Section 702, it must satisfy the statute's requirements, and the SIGINT Annex does not apply; if the government does not do so, then Section 702 does not apply and the SIGINT Annex may apply. The broad FISA exclusion in the SIGINT Annex is for "activities by the USSS that are conducted pursuant to FISA," a test that emphasizes actual use of the statute. SA § 1.2.b. (Other parts of the SIGINT Annex use language more directly tied to FISA's definitions, and the Annex does not suggest any reserved authority where the statute is preclusive or purports to define the exclusive means of conducting certain collection or targeting, although Presidents effectively may have done so in other settings in the past, see NSIP Chapter 15.)

For ELINT and FISINT (as opposed to COMINT), the Annex applies only to the extent that the activity in question "implicates the Fourth Amendment." SA § 1.2(a). This is understandable. By their nature, ELINT and FISINT – e.g., foreign radar signatures and/or missile telemetry – are far less likely than COMINT to involve information sent to, from, or about U.S. persons. The conventional understanding, based on *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), is that the Fourth Amendment has limited, if any, applicability to collection conducted abroad, targeting or concerning the activities of non-U.S. persons with no substantial, voluntary ties to the United States, who themselves are located abroad at or near in time to the collection. Seven Justices in *Verdugo* (all except Justices Brennan and Marshall) concluded that the Warrant Clause had no application in such cases. Four Justices in the majority concluded that the Reasonableness Clause likewise had no application because the relevant Fourth Amendment events – searches of Verdugo's homes in Mexico – were completed abroad and before his trial in the United States, at a time when he lacked the requisite connections to this country. See *id*. at 264. Justice Kennedy, the fifth vote, concurred, stating that his views "do not … depart in fundamental respects from the opinion of the Court, which I join," *id*. at 275, but then describing views that arguably did depart, whether or not fundamentally. Justice Kennedy agreed with the majority that lower "constitutional standards apply when the Government acts, in reference to an alien, within its sphere of foreign operations," *id*. at 277, expressly rejected application of the Warrant Clause in such cases, *id*. at 278, observed that a house search inside the United States would be subject to the Fourth Amendment, *id*., and finally voted to affirm Verdugo's conviction without specifically addressing the application of the Reasonableness Clause. The remaining four Justices in *Verdugo* (one concurring, two dissenting, and one in favor of a remand) all relied on Verdugo's (lawful, if involuntary) presence in the United States after the searches, as a criminal defendant, to conclude that (at least) the Reasonableness Clause applied to those searches. More recently, the Court has stated in the First Amendment context that "it is long settled as a matter of American constitutional law that foreign citizens outside U.S. territory do not possess rights under the U.S. Constitution." *USAID v. Alliance for Open Society Int'l*, 140 S. Ct. 2082, 2086 (2020).

Regardless of whether non-U.S. person SIGINT targets abroad have Fourth Amendment rights in some cases, cf. *Ibrahim v. DHS*, 669 F.3d 983 (9th Cir. 2012), their U.S. person interlocutors (and/or perhaps interlocutors of any nationality who are located in the U.S.) may have such rights in the incidental collection of their communications with the targets, in the unintentional (inadvertent) collection of their communications due to error, and/or in the

querying of databases with their identifiers. Cf. *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019) (upholding incidental collection, and discussing unintentional collection and querying, under FAA § 702). This is an important aspect of the SIGINT Annex and its rules for processing, querying, retention, and dissemination of COMINT information. As noted above, incidental collection of U.S. person communications as part of ELINT and FISINT is a remote possibility.

One of the emerging challenges for the SIGINT Annex – and for regulation of surveillance in general – may be a possibly growing divergence between the Fourth Amendment and statutory factors that govern electronic surveillance, including those in FISA. In *Hasbajrami*, for example, the court upheld FAA § 702 against a claim that it was unconstitutional because it involved the assistance of an electronic communication service provider in the United States under 50 U.S.C. § 1881a(h)(2)(A)(vi). The court explained that "[w]hat matters, and what implicates the protection of the Fourth Amendment, is the expectation of privacy in the communications themselves … [rather than] the physical location of the intercepting device … At least where the communication is collected essentially in real time as it occurs, the targeted communication, whether conducted over telephone wires or via the internet, occurs in the relevant sense where the person whose calls or emails are being intercepted is located, regardless of the location of the means used to intercept it." 945 F.3d at 665.

Decisions interpreting the Wiretap Act, however, have reached exactly the opposite conclusion. In *Huff v. Spaw*, 794 F.3d 543, 547 (6th Cir. 2015), which involved an accidental pocket dial from the plaintiffs in Italy to the defendant in the United States, the court concluded that the "relevant location … is not where the [plaintiffs'] conversations took place, but where [the defendant] used a device to acquire the contents of those conversations." A similar analysis likely applies to FISA, which as noted above defines "electronic surveillance" in part based on where acquisition occurs (50 U.S.C. § 1801(f)(2)) or where a surveillance device is installed or used (50 U.S.C. § 1801(f)(4)).

Congress may, of course, regulate above the constitutional floor in any way that it sees fit. A problem could arise, however, if FISA's definitions of "electronic surveillance" fall below that floor. For example, 50 U.S.C. § 1801(f)(2) and (f)(4) apply only if acquisition using a surveillance device "occurs," or such a device is "install[ed] or use[d]," "in the United States." Where the device is abroad but the surveillance targets are in the United States – e.g., something like a cross-border version of *Kyllo v. United States*, 533 U.S. 27 (2001), or the collection scenario in *Huff v. Spaw* but with the parties' locations reversed – the collection could fall outside of FISA but still raise very significant Fourth Amendment issues.

In the cross-border *Kyllo* scenario, of course, if use of the thermal imager from Mexico were not "electronic surveillance" under FISA, it would likely be a "physical search" because it would qualify as an "examination of the interior of property by technical means" occurring "within the United States" based on the domestic location of the home. 50 U.S.C. § 1821(5). But acquisition of other emanations, such as sound waves using a directional microphone, or the reciprocal of *Huff v. Spaw*, might fall outside the scope of both "electronic surveillance" and a

"physical search." The CIA's procedures that are analogous to the SIGINT Annex (available here and discussed in detail here) provide (in § 4.4.1.2) that "[w]hether a physical search occurs within or outside the United States depends on several factors, including the location of the item being searched and the location where the item came into the CIA's possession. For example, the search of a computer located abroad is a search outside of the United States, regardless of the location of the CIA employee conducting the search."

Finally, it is worth noting one other limit on the scope of the SIGINT Annex. It does not appear to regulate collection of data through something like a commercial transaction – e.g., buying information from a data broker. The DOD Manual and the SIGINT Annex treat the purchase of data as "collection," because it involves "information obtained or acquired by any means, including information that is volunteered" to the government by a third party, DOD Manual § G.2; SA § G.2, but the Annex understandably does not appear to treat such collection as "SIGINT" (as opposed to OSINT, HUMINT, or another intelligence discipline). Also, the SIGINT Annex is focused on activities regulated by the Fourth Amendment and buying data on the open market generally may not be regulated by the Fourth Amendment, at least assuming the data were properly collected and offered for sale. Applicable statutes tend to apply only when the collection involves a "surveillance device," 50 U.S.C. §§ 1801(f)(1)-(4), 1809, 1812; 18 U.S.C. §§ 2510(4)-(5), 2511(1), or when the entity providing the information is a provider of electronic communications service (ECS) or remote computing service (RCS), see 18 U.S.C. §§ 2702(a); cf. 18 U.S.C. § 2511(2)(f). If the government purchases data (rather than acquiring data with a surveillance device) from an entity other than an ECS or RCS, the collection may not be regulated by these statutes (where the data implicate First Amendment concerns – e.g., web browsing history – the Privacy Act might also come into play). Accordingly, the DOD Manual and the SIGINT Annex define data that are "available to the public by subscription or purchase" as "publicly available information," DOD Manual § G.2; SA § G.2, and the DOD Manual provides general authority to collect publicly available information, including USPI, if "necessary for the performance of an authorized intelligence mission or function assigned to" the DOD component in question. DOD Manual § 3.2.c. As I wrote in an analysis of the CIA's OSINT rules in 2017:

> With respect to intentional acquisition of "publicly available information" concerning a U.S. person, which qualifies as a "basic" collection technique, the CIA guidelines generally do not require any special approvals (although an authorized purpose is still required, and collection of very large quantities of publicly available information concerning U.S. persons is subject to additional restrictions under Sections 5 and 7 of the guidelines, as discussed further below). See CIA guidelines §§ 4.2(a), 4.21. As noted above, the key requirements with respect to such collection are that it must be for an authorized purpose, such as foreign intelligence or counterintelligence, and limited to information reasonably necessary to support that purpose. The same is true under the DOD procedures, see DOD Manual § 3.2.c(1), and was true under the prior CIA guidelines, see AR 2-2 § I.1.a(4)(c)(1)….
>
> [T]he DOD procedures … contain no explicit mention of "bulk collection," but they do call for additional requirements for "Special Circumstances Collection" depending on the

"volume, proportion, and sensitivity of USPI likely to be acquired, and the intrusiveness of the methods used to collect the information." DOD Manual § 3.2.e. When "special circumstances exist, the DOD component head or delegee must determine whether to authorize the collection and, if so, whether enhanced safeguards are appropriate." *Id*.

With a mission and function of performing SIGINT, rather than OSINT, it is not clear that the USSS would have authority to purchase data unless the data were related to a SIGINT mission (e.g., used to enhance information obtained through SIGINT, see SA § 3.2.a.(4)). In general, however, the DOD Manual seems to encourage collection from the open market over collection using SIGINT, considering the former to be less intrusive than the latter. See, e.g., DOD Manual § 3.5.(f)(3). This is important because, as noted above, one of the main technological developments of the post-9/11 era has been the relative improvement of the private sector, as compared to government, in ability to generate, access, collect, process, analyze and exploit data, including location data and other data about end users of devices or services. Vast amounts of data, including location data, are collected and available for sale by various private entities. Any possible future regulation in this area presumably would need to balance concerns about U.S. government access to such information against competing concerns that, if U.S. government access is limited by law, continued access would remain available to adversary foreign governments, commercial entities, and non-governmental organizations. Looking at the issue from the other direction, I have written about the counterintelligence concerns with such data being available – including, "as the range of social media and other publicly available information expands," possible difficulties "establish[ing] digital personae for undercover agents and officers" – and Congress also seems recently to have expressed some similar concerns.

b. *U.S. Person Presumptions*. To apply the SIGINT Annex, government officials need to know if the target of collection is or is not a U.S. person. Section 1.3(a) of the Annex follows the traditional approach in providing that anyone who is physically located in the United States will be presumed to be a U.S. person, and that the opposite presumption will apply to anyone located abroad. See, e.g., Section 3(j) of NSA's 2019 FAA 702 Minimization Procedures ("A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence or circumstances give rise to a reasonable belief that such person is not a United States person … A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such or circumstances give rise to a reasonable belief that such person is a United States person")). As I have written elsewhere, increasing international travel, and the increasing indeterminacy of location of persons using digital networks, makes these presumptions much less accurate and useful than they used to be. The U.S. government has not yet devised a replacement paradigm (and it is not clear that one can be devised).

The SIGINT Annex also provides, however, that the USSS may not simply rely on the location-based presumption. Instead, it requires "reasonable steps to determine the non-U.S. person status and location of a current or potential target." SA § 2.2.a.(3). These "reasonable

steps" may in some cases be comparable to the diligence required under Part I of NSA's FAA § 702 Targeting Procedures. An earlier version of those Targeting Procedures was described by the PCLOB as follows:

> The government has stated that in making this foreignness determination the NSA targeting procedures inherently impose a requirement that analysts conduct "due diligence" in identifying these relevant circumstances. What constitutes due diligence will vary depending on the target; tasking a new selector used by a foreign intelligence target with whom the NSA is already quite familiar may not require deep research into the target's (already known) U.S. person status and current location, while a great deal more effort may be required to target a previously unknown, and more elusive, individual. As previously discussed above, a failure by an NSA analyst to conduct due diligence in identifying relevant circumstances regarding the location and U.S. person status of a Section 702 target is a reportable compliance incident to the FISC.
>
> After conducting due diligence and reviewing the totality of the circumstances, the NSA analyst is required to determine whether the information indicates that the target is a non-U.S. person reasonably believed to be located outside the United States. The government has stated, and the Board's review has confirmed, that this is not a "51% to 49% test." If there is conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting.

Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 43-44 (July 2, 2014) (footnotes omitted, emphasis added).

2. COLLECTION

Section 2 of the SIGINT Annex regulates the first operational step in the intelligence lifecycle: collection of information. Read without a firm understanding of the Annex's scope, it might (wrongly) suggest an alarming breadth. The discussion of Section 2 below therefore frequently cross-references the discussion above concerning Section 1 of the Annex, including the FISA exclusion.

Structurally, Section 2 proceeds logically enough. It begins with the authorized purposes for SIGINT collection (§ 2.1), imposes certain general requirements such as rules for determining the U.S. person status of surveillance targets (§ 2.2), and then describes in a series of subsections several considerations (§ 2.3), prohibitions (§ 2.4), limitations (§ 2.5), and exceptions to those limitations (§ 2.6) for SIGINT collection. Each of those subsections is reviewed below. In some cases, by imposing a particular limit or prohibition on SIGINT, the Annex reveals something by negative implication about the scope of permitted SIGINT, and functions more like an affirmative authorization; the discussion below attempts to highlight

those cases. Indeed, the six categories within Section 2 may make sense only because of legacy regulations and operations; they are very complex and highly interrelated in ways that are not always obvious.

Purpose. Section 2.1 of the Annex provides, under the heading "scope," that Section 2 as a whole "governs SIGINT collection by the USSS under E.O. 12333" for three purposes: "to satisfy foreign intelligence or counterintelligence requirements, to provide support to military operations," or in certain circumstances "to protect the safety or enable the recovery of a U.S. person captive." (As discussed below, very similar language describes the authorized purposes for querying in SA §§ 3.3 and 3.5.)

The first two authorized purposes are easy to understand. As to the first, intelligence and counterintelligence are the bread and butter of the Intelligence Community by statute (e.g., 50 U.S.C. §§ 3002, 3003), executive order (e.g., EO 12333 § 1.7(c)), and related regulations (e.g., DOD 5100.20). The first purpose, "to satisfy foreign intelligence or counterintelligence requirements," is therefore entirely sensible. Of course, the details of intelligence and counterintelligence requirements are not self-evident; they are determined through procedural mechanisms such as the National Intelligence Requirements Framework. See, e.g., ICD 204. But it is almost axiomatic to say that signals intelligence collection may be conducted for the purpose of meeting those requirements.

The second authorized purpose for SIGINT collection, "to provide support to military operations," is also easily understandable. The USSS includes military SIGINT components and (as noted above) NSA itself is both a "Combat Support Agency of the Department of Defense" and "an element of the Intelligence Community (IC) subject to the oversight of the DNI," DOD 5100.20 § (5)(b) & (e). It is therefore not surprising that the authorized purposes for SIGINT collection include support of military operations. Authorized military operations may expand or contract depending on the circumstances, see, e.g., 10 U.S.C. § 252, or direction from the Commander in Chief, but at the conceptual level it makes sense for the USSS to support our nation's warfighters. In general terms, the first two purposes in Section 2.1 of the SIGINT Annex ensure that SIGINT collection is aligned with authorized intelligence or defense activity.

The third purpose listed in Section 2.1, concerning hostage rescue, is in keeping with tradition and intuitively appealing, but arguably redundant. It provides (§ 2.5.c.) that the "USSS may provide SIGINT support for national and departmental requirements and for the conduct of military operations … when the collection is not governed by FISA and is necessary to protect the safety or enable the recovery of a U.S. person held captive outside the United States" under certain conditions and limitations. In general, "when a U.S. person outside the United States is reasonably believed to be held captive by a foreign power or other non-U.S. person, the USSS may intentionally collect SIGINT information that is necessary to protect the safety or enable the recovery of that person." SA § 2.5.c.(1). Such collection may even "target[]" the U.S. person captive, but only "for the purpose of supporting … the safety or recovery of the U.S. person captive" and only to acquire a limited range of information about the captive's location and condition, the degree of risk associated with conducting an operation or facilitating the U.S.

person's escape, and the identities, affiliations, and vulnerabilities of the captors. SA § 2.5.c.(2). Collection for the purpose of hostage rescue does not permit targeting any U.S. person other than the captive or any non-U.S. person located in the United States. SA §§ 2.5.c.(2)(b), (3).

The IC has long collected intelligence concerning U.S. persons reasonably believed to be held captive abroad by foreign persons or entities. Collection for that purpose was addressed in NSPD-12, issued by President Bush in 2002, and in PPD-30, issued by President Obama in 2015. It was emphasized recently in a Memorandum on Authority of the Intelligence Community to Collect Certain Intelligence Regarding United States Persons Held Captive Abroad, issued by President Trump on September 30, 2020. Under the Prior Annex, intentional collection of communications "of or concerning a United States person" was permitted "in any case in which the United States person is reasonably believed to be held captive by a foreign power or by a group engaged in international terrorist activities." Prior Annex § 4.A.1 at page A-5.

There is certainly an intuitive appeal to the idea that, if a U.S. person is taken hostage abroad, the IC will attempt to locate the person and collect SIGINT in aid of recovery. In the context of Section 2.1 of the SIGINT Annex, however, the provision appears to be redundant because it provides only that the "USSS may provide SIGINT support for national and departmental requirements" connected to hostage rescue. SA § 2.5.c. Precisely to the extent of those requirements, SIGINT support for hostage rescue would seem to be permitted under the first two authorized purposes – "to satisfy foreign intelligence or counterintelligence requirements [and] to provide support to military operations" – and beyond them by its terms the hostage authorization adds nothing. From the perspective of operational personnel, it may be useful to emphasize in Section 2.1 that hostage rescue is a valid purpose for SIGINT collection, and/or to expressly cross-reference the limits on SIGINT collection for that purpose in Section 2.5.c. If so, however, it is not clear why Section 2.1 does not also cross-reference (pre-existing) SIGINT collection authority in support of efforts against international drug trafficking, transnational organized crime, and illicit communications as set forth in Section 2.6, or other situations involving exigent circumstances as authorized in SA § 2.5.b.3. The SIGINT Annex would benefit from a single, comprehensive statement of the purposes for which SIGINT collection, and other SIGINT activity, may (and may not) be conducted. Under Section 3.f.(2) of the DOD Manual, a "Defense Intelligence Component may not collect USPI solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States." Under Section 1(b) of PPD-28, the "United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion," and SIGINT "shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes."

General Requirements. Section 2.2.a of the Annex provides that the USSS generally may collect SIGINT "inside or outside the United States by any lawful means," but that it may not "intentionally target U.S. persons or persons in the United States unless authorization has been obtained in accordance with this section or FISA." This language sets a narrower aperture for

collection than might appear at first glance, principally because – as discussed above – FISA occupies much of the field of SIGINT conducted inside the United States, including but not limited to SIGINT intentionally targeting U.S. persons or persons in the United States. The SIGINT Annex cannot and does not purport to override FISA requirements. See SA § 1.2.b. When FISA applies, the SIGINT Annex directs the USSS to follow FISA, as it should. This is consistent with Procedure 5 of the DOD Manual and Section 2.5 of Executive Order 12333, the SIGINT Annex's parent and grandparent documents, which provide expressly for adherence to FISA.

As noted above, however, there are situations in which SIGINT conducted inside the United States, including such SIGINT targeting U.S. persons, is not regulated by traditional FISA. For example, acquisition of transiting wire communications in the U.S., even if sent to and from U.S. persons abroad, is not regulated by traditional FISA (it is regulated by FAA § 704 if one of the U.S. persons, or any other U.S. person located abroad, is intentionally targeted). Similarly, acquisition of international radio communications, including such acquisition when conducted inside the United States, is not regulated by traditional FISA unless a particular U.S. person in this country is intentionally targeted (it may be regulated by FAA § 704 if the intentionally targeted U.S. person is located abroad). Where the SIGINT collection is not regulated by FISA, the SIGINT Annex sets requirements (some of which are analogous to those in FISA).

With respect to the non-FISA forms of SIGINT collection that it regulates, Section 2 of the Annex requires (§ 2.2.a(1)) that the USSS "limit SIGINT collection" of USPI to "collect no more information than is reasonably necessary" under DOD Manual 3.2.f.(4), and perhaps also to use the least intrusive means feasible. See DOD Manual § 3.2.f.(3) (cross-referenced by § 3.2.f.(4)). (There may be some question as to whether the "least intrusive means" prescription governs not only whether to conduct SIGINT as opposed to some other form of collection, but also how SIGINT is conducted.) In any event, under Section 2.4 of Executive Order 12333, "[e]lements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad," and Section 1(d) of PPD-28 provides that all SIGINT "activities shall be as tailored as feasible," prioritizing other methods of gaining intelligence where feasible. Although the SIGINT Annex is explicitly focused on protecting U.S. persons (and persons of any nationality in the United States), it also contains some important limits that protect non-U.S. persons abroad, as noted in Part III.

The SIGINT Annex requires the USSS to use targeted collection (as opposed to bulk collection) "whenever practicable." SA § 2.2.a.(2). This is normally accomplished with the use of selection terms or other discriminants that are designed to limit collection "to the greatest extent reasonably practicable." SA § G.2. However, the USSS may use broader discriminants (i.e., discriminants not designed to limit collection to the greatest extent practicable) or even engage in "bulk collection when necessary due to technical or operational considerations." SA § 2.2.a.(2). Here too, the Annex might suggest broader collection than is actually possible, because PPD-28 and its subordinate procedures, which remain in effect, provide that "bulk collection" (defined identically in PPD-28 footnote 5 and in SIGINT Annex § G.2) is available only for six specific purposes (PPD-28 § 2):

> when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.

Moreover, PPD-28 provides (§ 2), "[i]n no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; affording a competitive advantage to U.S. companies and U.S. business sectors commercially; or achieving any purpose other than those identified in this section."

Under Section 2.2(a)(3), the USSS must take "reasonable steps" to determine the nationality and location of targets. This informs the application of appropriate rules, which often depend on nationality and location of targets.

Finally, under Section 2.2.b, the USSS must "make every reasonable effort … to reduce, to the maximum extent possible, the number of … incidentally collected communications" that are domestic or that concern (are to, from or about) U.S. persons. As discussed below, there are rules governing processing, retention, and dissemination of such incidentally collected information in other parts of the SIGINT Annex.

Considerations. Section 2.3 of the Annex provides that in "conducting collection" and in developing "collection techniques," the USSS "will consider" several factors, and will also "consider whether additional approvals" or "protections" for privacy and civil liberties are required. SA 2.3.a-b. The requirements are only to "consider" the listed factors. But in basic approach here the Annex is not too far removed from FISA minimization requirements, which fundamentally require a balancing of U.S. foreign intelligence needs against U.S. person privacy interests (albeit with the particular balance reviewed and approved by the FISA Court). See, e.g., 50 U.S.C. §§ 1801(h), 1805(a)(3). The considerations are as follows (SA § 2.3.a.):

(1) Methods to limit collection of non-pertinent information that identifies a U.S. person (USPI).

(2) Methods to limit other types and aspects of non-pertinent information.

(3) If non-pertinent information is collected, whether it can be filtered "as soon as practicable after collection." (This is discussed further in the section on processing and querying below.)

(4) Whether the collection is sensitive "based on the volume, proportion, and sensitivity of the USPI likely to be acquired" under DOD Manual 3.2.e ("special circumstances" collection).

In addition, the USSS must also consider whether "additional approvals or civil liberties and privacy protections are needed." SA § 2.3.b.

Prohibitions. Apart from the "considerations" described above, the Annex includes in Section 2.4 a general prohibition that the USSS "will not intentionally collect domestic communications." SA § 2.4.a. There are three specific exceptions to this general rule. First, of course, FISA, which clearly authorizes intentional collection of domestic communications under certain circumstances. SA § 2.4.1.(3). Second, where authorized under Sections 3.5.i, j, or k of the DOD Manual. SA § 2.4.1.(2) These sections of the DOD Manual apply to training and testing of personnel or equipment, technical surveillance countermeasures (TSCM), "Transmission Media Vulnerability and Radio Communications Hearability Surveys," and "Military Tactical Exercise Communications." These are generally outside of FISA either by specific exemption – e.g., for training and testing under 50 U.S.C. § 1805(g), or via consent that removes the collection from the definition of "electronic surveillance." Third, domestic communications may be intentionally collected when authorized under the "Limitations" provisions in Section 2.5 of the Annex, which is discussed next.

Limitations. Section 2.5 of the Annex sets out several categories of limitations on SIGINT collection: (a) limitations on certain collection methods; (b) limitations on collection targeting U.S. persons; (c) special rules concerning U.S. person captives; and (d) limitations on collection targeting non-U.S. persons in the United States. There are at least three significant challenges in understanding what these limitations mean.

First, the limitations are very carefully and densely worded and require considerable unpacking to explain. This is not necessarily a shortcoming, because the SIGINT Annex is mainly designed to help operational personnel comply with the law, and excessive explanation might not be necessary for them, and could make the document longer and more cumbersome.

Second, although they are labeled "limitations," many of them also function as affirmative authorizations for certain kinds of SIGINT collection. For example, the limitations pertaining to U.S. person captives (SA § 2.5.c) may function effectively as an authorization for SIGINT as discussed above.

Third, the limitations address the intersection between the Annex and FISA in different ways: sometimes they describe scenarios which, were it not for an explicit or implicit prior exclusion of collection activity governed by FISA, would conflict with the statute; sometimes they describe scenarios that are, as described, not governed by FISA, but the Annex does not say so explicitly; and sometimes they describe scenarios that, as described, are governed by but would comply with FISA, again without saying so explicitly.

The overriding goal in all cases seems to be to help SIGINT analysts or collectors comply with legal requirements – whether FISA or the Fourth Amendment – but the legal background for and provenance of the limitations is not always as obvious or explicit as it might be, at least to an outsider. In some cases, certain of these challenges may be the product of efforts to maintain continuity with legacy SIGINT regulations that were developed long ago, and before the FISA Amendments Act, again perhaps for the benefit of operational personnel.

(a) Limitations on Certain Collection Methods. Section 2.5.a of the SIGINT Annex imposes limitations on two major kinds of SIGINT collection methods. First, there are limitations on collection using "selection terms" or other discriminants. Second, there are limitations on collection "surveys." SA § 2.5.a.(1)-(2).

(i) Limitations on Using Selection Terms. As noted above, the USSS is authorized and encouraged to collect SIGINT using "selection terms." SA §§ 2.2.a.(2); 2.5.a.(1). Under the Annex (SA § G.2), a selection term is the

> composite of individual terms used to effect or defeat the collection or querying of particular communications, information, or data of interest. It comprises the entire term or series of terms so used, but not any segregable term contained therein. A selection term limits, to the greatest extent reasonably practicable, the scope of the information sought, consistent with the purpose of the collection or query.

For purposes of the Annex, selection terms may "identify a target, a subject matter or a characteristic of the communication or a combination of these elements, or other discriminants." SA § 2.5.a.(1). A selection term "limits, to the greatest extent reasonably practicable, the scope of the information sought, consistent with the purpose of the collection or query," SA § G.2, but there is no requirement in the Annex, as there is in FISA, for a selection term to "specifically identif[y] a person, account, address, or personal device." 50 U.S.C. § 1841(4)(A). A selection term therefore is not the same as a strong "selector," a word used in other contexts to designate a facility like a specific email address or telephone number.

To take a simple and fanciful example of a "selection term" as an illustration, the Annex would permit the use of a combination of selection terms like this: any message that (1) contains the word "wherefore" used within three words of the phrase "art thou"; (2) is more than 85% written in iambic pentameter; and (3) is transmitted between 9:00 AM and 5:00 PM GMT. Cf. *In re [redacted] Non-U.S. Persons*, No. 19-218 (FISC March 5, 2020).

William Shakespeare was a non-U.S. person, but where selection terms "are reasonably likely to result in, or have [when used in the past] resulted in, the collection of communications to, from, or about U.S. persons (wherever located)," the Annex imposes additional requirements. SA § 2.5.a.(1). It is important to recognize that the selection terms in question here may in fact threaten U.S. person privacy interests, but in most cases, will not be designed to do so. Use of selection terms designed to acquire communications to, from, or about U.S. persons, or at least any particular U.S. persons, would amount to targeting them, which is in

most cases governed by traditional FISA, FAA § 704, and other parts of the SIGINT Annex, including the prohibitions in SA § 2.4 and limits in § 2.5.b. The threat to U.S. persons addressed in this part of the SIGINT Annex, in other words, is from incidental or unintentional acquisition.

When U.S. person privacy interests are threatened, the additional requirements in SA § 2.5.a.(1) apply. Those requirements involve some kind of filter or other mechanism "designed to defeat, as practicable under the circumstances, the collection of" communications or data related to those communications that are not pertinent to any of the Annex's three authorized purposes (foreign intelligence, support for military operations, and aiding U.S. person captives). SA § 2.5.a.(1). (A similar standard, without redactions, applies to querying collected data under SA § 3.3, as discussed below.)

NSA has used technical "defeat lists" and related "data reduction and management strategies" in other SIGINT settings, as explained in this document. The bottom line is that if NSA collects SIGINT using selection terms that threaten U.S. person privacy interests, it must take steps to ensure that non-pertinent communications are excluded. Cf. 18 U.S.C. § 3121(c) ("A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications." (emphasis added)).

After reviewing its general approach to the use of selection terms, the Annex describes two specific SIGINT collection scenarios that may involve the use of such terms. These scenarios are set out in subsections (a) and (b) of Section 2.5.a.(1), which suggests that they are both examples of situations in which U.S. person privacy interests might be threatened by the use of selection terms as described above. Both descriptions are redacted in part, however, so it is difficult to be sure.

The first scenario involves collection of "foreign radio communications" of some sort "that pass over a channel with a terminal in the United States." A "terminal" is not defined in the Annex, but it refers to an access point or endpoint. Under the SIGINT Annex, a communication is "foreign" if it has at least one end abroad, meaning that the term covers international communications with a terminal in the United States. SA § G.2. The same definition of a "foreign" communication applied under the Prior Annex (§ 2 at page A-2).

When monitoring such an international radio communications channel, the SIGINT Annex provides, the USSS will "target non-U.S. persons outside the United States," and must use selection terms (i.e., may not acquire all communications – engage in bulk collection – in the channel) except where the channel is used "exclusively by a foreign power." This is consistent with traditional FISA, which does not regulate acquisition of international radio communications (i.e., communications acquired from a radio wave) unless a particular U.S. person in the U.S. is being targeted. See 50 U.S.C. § 1801(f). It is also properly characterized as a

limitation on SIGINT collection: even though FISA does not prohibit bulk collection of international radio communications on a channel with a terminal in the U.S., the SIGINT Annex does so by requiring the collection to have a non-U.S. person target located abroad and also requiring the use of selection terms to accomplish the targeting. The unspoken premise for these limitations is that the radio channel may carry many communications, some (or perhaps most) of which are inappropriate for collection. Microwave relay stations on the ground, and communications satellites in orbit, use radio waves for communications in the United States, including in some cases for international communications, as explained by the FCC here and here.

The first scenario also refers to international radio communications in a channel that is used "exclusively by a foreign power." There is a narrow category of "electronic surveillance" that is permitted under traditional FISA without Court approval, based on a certification from the Attorney General. See 50 U.S.C. § 1802. Section 1802 applies (emphasis added) to "electronic surveillance" that is solely directed at "(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among [a governmental] foreign power[] … or (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of" such a foreign power, if "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party" and proper minimization procedures are in place. Although the SIGINT Annex uses a key phrase from Section 1802 to describe the scenario, as noted above the scenario does not appear to involve "electronic surveillance" as defined by FISA (because it involves collection of international radio communications not targeting a U.S. person), so Section 1802 does not actually apply. But the SIGINT Annex's grant of authority to eschew selection terms in channels used exclusively by foreign powers seems to rest on the same common-sense policy foundation as Section 1802.

To make sense of this first scenario, it helps to assess it in three layers. Begin with a traditional collection scenario in which the USSS is engaging in RF SIGINT collection targeting non-U.S. persons abroad – e.g., on a foreign governmental network. Normally, in that scenario, the USSS understandably enjoys considerable freedom of action. Where, however, the foreign network connects via RF channel to the United States, the Annex provides that the USSS must use selection terms and must be targeting non-U.S. persons located abroad. Finally, however, where the RF connection to the U.S. is used only by a foreign power – e.g., a dedicated link between foreign governmental establishments – then the requirement to use selection terms does not apply because the privacy concerns normally associated with monitoring communications to and from the U.S. are not present. It may be that the standards imposed by the SIGINT Annex here reflect an assessment of the requirements of the Fourth Amendment.

The second scenario involving selection terms is harder to discern because of more extensive redactions, but apparently applies to something "Used by a Foreign Entity" that has "a terminal in the United States that service a U.S. person." Unlike the first scenario, this collection scenario is not described as being limited to radio communications, and so it may

apply to the acquisition of wire communications or other things. Cf. Prior Annex § 4.A.1.(e) at page A-7.

Whatever it is, this second collection scenario requires a certification from DIRNSA or his delegee to the Attorney General. The certification must confirm three important elements: (1) "the target of the collection is a non-U.S. person outside the United States"; (2) the "collection technique does not fall within FISA's definition of electronic surveillance"; and (3) "the purpose of the collection is to obtain foreign intelligence or counterintelligence." This collection scenario, which explicitly excludes "electronic surveillance" as defined in FISA, does not appear to involve 50 U.S.C. § 1802 or 50 U.S.C. § 1881a (FAA § 702), but rather applies to collection by the USSS that is outside the scope of "electronic surveillance," perhaps including collection of foreign-to-foreign communications that transit this country and are acquired here from a "wire, able, or other like connection," 50 U.S.C. § 1801(*l*), and likely involving acquisition of international radio communications not targeting a U.S. person in the United States.

(ii) Limitations on Surveys. Apart from limitations involving selection terms, the second SIGINT collection method subject to limitations is a survey. A survey is what it sounds like – a review of "the signals environment" to identify "signals or communications" that are important for future collection. SA § 2.5.a.(2)(a). For persons of a certain age, at least, it may be analogized to turning the dial on a car radio to find the local stations that carry a particular kind of music or other programming (NSA itself makes this analogy). A survey may only be conducted to identify communications or other signals that meet at least one of the following four requirements (SA § 2.5.a.(2)(a)):

(1) "May contain information related to the production of foreign intelligence or counterintelligence." This is the most basic category for a survey. It involves the USSS hunting for communications that have direct intelligence value, such as messages between a forward deployed military unit or intelligence asset and its headquarters.

(2) "Are enciphered or appear to contain secret meaning and are needed to develop technical capabilities." Such communications may well have direct intelligence value, but the emphasis here appears to be on collecting information that can be used in efforts to break a cypher, apart from the substantive value of the particular coded message itself. For example, cryptanalysis of a particular military cipher used by an adversary may benefit from a large sample of enciphered data.

(3) "Are needed to ensure efficient SIGINT collection or to avoid the collection of unwanted signals." Surveys are important in a world of many communications channels and limited SIGINT resources. They allow NSA and other elements of the USSS to survey the larger environment in an effort to direct collection against the most valuable channels and to avoid dry holes. They also may permit identification of channels containing a large number or percentage of communications that are not appropriate for collection, informing decisions to avoid directing SIGINT against such channels.

(4) "Reveal U.S. communications security vulnerabilities." Surveys support affirmative intelligence gathering, but they are also relevant for counterintelligence and TSCM. For example, NSA might survey a channel with a terminal in a U.S. intelligence installation to check whether large quantities of sensitive data are being exfiltrated.

These four categories are consistent with historical practice. They are nearly identical to the "search and development" categories specified in Section 4.D (pages A-11 to A-12) of the Prior Annex, in Annex E to USSID-18 from 2011 and going back to at least 1993, and appear similar to the publicly-available language used in Annex F to the 1980 version of USSID-18.

The purpose and function of a survey is not to collect foreign intelligence in the first instance (although it may result in such collection), but to ascertain information about the SIGINT environment to facilitate such collection – i.e., to guide and inform SIGINT collection. Cf. Prior Annex § 3 (page A-5). Accordingly, a survey is not, and "must not be used as," a "substitute for sustained collection," and must be "reasonable and appropriately limited in scope, output, and duration." SA §§ 2.5.a.(2)(c), 2.5.a.(2)(b). Surveys may use selection terms to help identify whether a surveyed channel – e.g., a radio frequency – contains relevant information, but surveys of communications channels with a terminal (i.e., an access point or endpoint) in the U.S. may be conducted only to "determine whether the channel contains" intelligence, must be as limited in duration as possible in keeping with that purpose, and, if the survey does not involve selection terms, must not exceed two hours without special approval. SA § 2.5.a.2.(c)(1)-(2). Some of these limits on surveys in the SIGINT Annex appear to be more strict, or at least more explicitly stated, than those in the Prior Annex.

A survey may not involve "electronic surveillance as defined by FISA, unless the survey is otherwise permitted by FISA" (and also permitted by Procedure 5 of the DOD Manual, which generally cross-references FISA). SA § 2.5.a.2.(c). As noted above, FISA's definition of "electronic surveillance" excludes a few acquisition scenarios in the United States, such as acquisition of transiting wire communications and international radio communications as to which there is no particular U.S. person target located in the United States. The statute has much reduced reach and preclusive effect as applied to SIGINT collection conducted abroad that does not target a U.S. person.

It is difficult to identify situations in which a survey might qualify as "electronic surveillance" and still be "otherwise permitted by FISA," and it may be that this language in the Annex is meant mainly to remind operational personnel that surveys are not *per se* exempt from FISA. By its nature, because a SIGINT survey does not involve a target or any purpose directly to collect foreign intelligence information, it is not something for which the FISA Court could grant an authorization order under traditional FISA, 50 U.S.C. §§ 1805, or FAA § 704, 50 U.S.C. § 1881c, and it is not something that could be permitted under the NSA's targeting procedures and other rules associated with collection under FAA § 702, 50 U.S.C. § 1881a. Putting aside SIGINT during the 15 days immediately following a declaration of war, see 50 U.S.C. § 1811, there might be three unusual situations in which FISA could authorize "electronic surveillance" that is plausibly relevant to a SIGINT survey, but none of them is very likely.

The first situation, discussed above, is for SIGINT that has "no substantial likelihood" of acquiring a U.S. person's communication and that is "solely directed at" the communications of governmental foreign powers or "the acquisition of technical intelligence" from an embassy or other "property under the open and exclusive control" of such foreign powers. See 50 U.S.C. § 1802. This type of collection can be accomplished on a certification from the Attorney General without the approval of the FISA Court. It is possible that NSA would want to conduct surveys within the range of collection permitted by Section 1802 as a matter of resource-allocation, focusing attention on the channels that are most likely to yield valuable information. But channels used solely by foreign powers may be worth monitoring without the need for a survey, and such channels may not qualify as an "environment" in which to conduct a survey.

The second possible situation related to a survey in which "electronic surveillance" as defined by traditional FISA could be permitted by FISA is for training and testing surveillance personnel and equipment or to detect unauthorized surveillance. See 50 U.S.C. § 1805(g). Under certain conditions, FISA authorizes "electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to" do one or more of three things: (1) "test the capability of electronic equipment"; (2) "determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance"; and (3) "train intelligence personnel in the use of electronic surveillance." 50 U.S.C. § 1805(g). It is conceivable that NSA would conduct a SIGINT survey within these parameters. But training and testing seems to be regulated separately from surveys in Section 3.5.i of the DOD Manual, so this possibility may not be relevant. Cf. USSID-18 Annex G.

The third and final situation that might conceivably qualify here would be the use of a packet-sniffer to scan the dialing, routing, addressing, or signaling information (DRAS) of packets passing through a high-capacity transmission channel or channels. This type of collection would qualify as "electronic surveillance" under FISA (because FISA defines "contents" to include DRAS, see 50 U.S.C. § 1801(n)), might be authorized under FISA's pen register provisions, see 50 U.S.C. § 1841 et seq., and might conceivably be treated as a survey to the extent that all of the packets in the channel or channels were being sampled briefly for the appropriate DRAS characteristics. But again, it does not seem very likely.

Even if they do not reveal much about surveys, the foregoing three situations may be useful to consider insofar as they illustrate the difficulties that outsiders may have interpreting new policy documents in a classified environment.

(b) Limitations on Collection Targeting U.S. Persons. Under Section 2.5.b of the SIGINT Annex, the USSS "may intentionally target a U.S. person, whether inside or outside the United States, only" in very limited circumstances. Chief among these limited circumstances is "if the collection is not governed by FISA." The reference to FISA here is worded differently than references in other parts of the SIGINT Annex, e.g., SA § 2.5.a.(2)(c) (USSS may not "engage in electronic surveillance as defined by FISA"); SA § 1.2.b. (SIGINT Annex "does not govern

activities by the USSS that are conducted pursuant to FISA"), but it does not appear that any different meaning is intended. Again, therefore, if SIGINT collection would be "electronic surveillance" or a "physical search" as defined by FISA, or if it is in fact conducted under FAA § 702 (not possible where the target is a U.S. person), it is excluded from this part of the SIGINT Annex and must comply with the statute; if it is subject to FAA § 704 then it must comply with Appendix 7A to the Annex and the statute.

In addition to requiring that SIGINT collection targeting a U.S. person be ungoverned by FISA, the Annex also requires one or more of three additional circumstances. For the most part, these three circumstances appear to describe specific ways of ensuring that FISA does not apply or that it is satisfied, and/or that the Fourth Amendment is satisfied.

The first identified circumstance, SA § 2.5.(b)(1), applies where there is an appropriate, case-specific consent to the SIGINT collection. Such consent removes a collection scenario from regulation by FISA because the definitions of "electronic surveillance" are written such that they apply only to acquisition "without the consent of any party" to a communication, 50 U.S.C. § 1801(f)(2), or "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes," 50 U.S.C. §§ 1801(f)(1), (3), (4), 1821(5). Consent to a surveillance or search removes the requirement for a law enforcement warrant. See 18 U.S.C. § 2511(2)(c); *Lopez v. United States*, 373 U.S. 427 (1963). A standard consent form is included in Annex H to USSID-18 but may not endure the forthcoming revision to that document. By describing this circumstance, the SIGINT Annex helps operational personnel understand whether and how FISA applies, and does not apply, to a collection scenario.

Another of the three identified circumstances, SA § 2.5.(b)(3), also brings a SIGINT collection scenario out from under FISA, at least as far as the U.S. government is concerned. It is a cross-reference to Section 3.5.(h) of the DOD Manual, which applies to collection in exigent circumstances targeting a U.S. person outside the United States. Under DOD Manual § 3.5.(h), where it is not practical to secure the Attorney General's approval, upon the approval of a high-ranking defense official, the USSS may target a U.S. person abroad when "a person's life or physical safety are reasonably believed to be in imminent danger." It may also do so with the requisite approvals when the U.S. person target meets the relevant definitions in FAA § 704, and either (1) a defense installation or other government property is in imminent danger, or (2) the time required to obtain AG approval "could cause failure or delay in obtaining significant foreign intelligence" or counterintelligence, and the failure would "result in substantial harm to the national security." The theory here is that FAA § 704 applies only where "the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes," 50 U.S.C. § 1881c(a)(2), and exigency eliminates the warrant requirement. See, e.g., *Mincey v. Arizona*, 437 U.S. 385, 394 (1978). The exigency elements of DOD Manual § 3.5 bear an interesting relationship to the emergency provisions of FAA § 704, 50 U.S.C. § 1881c(d), which also may rely on a theory of exigency, particularly as a scenario endures for a long period of time. See NSIP § 2:7 (at pages 59-60). Again, however, this second scenario may be included in

the SIGINT Annex as a way of advising operational personnel whether and how FISA applies, and does not apply, to certain collection scenarios. This is an appropriate and helpful function for the Annex to aid operational personnel in a complex regulatory environment.

The last additional circumstance identified in the SIGINT Annex, SA § 2.5.b.(2), is analogous to the requirements in FAA § 704. It applies where the "Attorney General determines" that there is "probable cause" that the U.S. person is an "agent of a foreign power or an officer or employee of a foreign power," and where the purpose of the collection is "to acquire significant foreign intelligence or counterintelligence." The first part of this standard mirrors the central requirements in FAA § 704, 50 U.S.C. § 1881c(b)(3)(B), and the pre-FAA language of Section 2.5 of EO 12333. Again, however, the scenario only applies where the collection is not governed by FISA, so this is not an attempt to substitute the Attorney General for the FISA Court, which must approve all collection under FAA § 704 absent an emergency. See 50 U.S.C. § 1881c(d). That intent is confirmed by the second part of the Annex's standard, which uses terms that are familiar to the Intelligence Community based on Executive order 12333 § 3.5(a), (e), and (f), and 50 U.S.C. § 3003(1)-(3), but slightly different from their closest analogue in FISA – "foreign intelligence information" as defined in 50 U.S.C. § 1801(e) – and therefore clearly not meant to satisfy the statute. See 50 U.S.C. § 1881c(b)(5). This scenario is the SIGINT Annex imposing on non-FISA collection a set of standards that are analogous to those applicable to FISA collection, perhaps to ensure compliance with the Fourth Amendment.

(c) Limitations Concerning U.S. Person Captives. As noted above in the discussion of Section 2.1, Section 2.5.c of the SIGINT Annex allows the USSS in certain circumstances to "provide SIGINT support for national and departmental requirements" – i.e., for civilian intelligence and military requirements – "when the collection is not governed by FISA and is necessary to protect the safety or enable the recovery of a U.S. person held captive outside the United States." The gist of the provision is that the USSS may target a U.S. person abroad, in the absence of any derogatory information about him (e.g., in the absence of any information suggesting that he is an agent of a foreign power), for the purpose of saving his life from non-U.S. persons who have kidnapped him.

The SIGINT Annex explains the scope and reason for the authorization: "[w]hen a U.S. person outside the United States is reasonably believed to be held captive by a foreign power or other non-U.S. person, the USSS may intentionally collect SIGNT information that is necessary to protect the safety or enable the recovery of that [U.S.] person." SA § 2.5.c.(1). When it comes to targeting the U.S. person – e.g., directing surveillance against his mobile telephone – the collection "must be for the purpose of supporting national or departmental requirements or the conduct of military operations concerning the safety or recovery of the U.S. person captive," and also must be limited to five defined categories of information, such as the captive's location, his physical and mental condition, the degree of risk associated with escape or recovery, the identities and affiliations of his captors, and the captors' vulnerabilities. SA § 2.5.c.(2)(a)(1)-(5). Such collection is permitted only with the approval of DIRNSA or a delegee for periods of up to 90 days at a time, SA § 2.5.c.(4), and with notice to the Department

of Justice, SA § 2.5.c.(5). This part of the Annex does not confer authority to target any U.S. person except the captive, or any non-U.S. person in the United States. SA § 2.5.c.(2)(b), (3).

The captive standard in the SIGINT Annex is, on its face, both broader and narrower than the analogous standard set in the Prior Annex, which allowed intentional collection of communications "of or concerning a United States person … in any case in which the United States person is reasonably believed to be held captive by a foreign power or by a group engaged in international terrorist activities." Prior Annex § 4.A.1 at page A-5. The SIGINT Annex is broader than the Prior Annex insofar as it applies to all non-U.S. person captors, not merely to foreign powers or terrorists. But it is narrower than the prior Annex in that it limits the scope of the collection targeting the U.S. person. On the other hand, both the current DOD Manual and its predecessor authorize(d) collection in emergency situations involving a U.S. person abroad. See DOD Manual § 3.5.h.; Prior DOD 5240.1-R § C5.2.4. Indeed, the Prior Annex's hostage provision included an express cross-reference to that DOD authorization. Prior Annex § 4.A.1.(d)(1) (page A-6). The SIGINT Annex does not include such a cross-reference in Section 2.5.c., but it does do so in Section 2.5.b., which as noted above purports to describe the "only" situations in which a U.S. person in any location may be targeted. As a result, it is not clear how significant the facial differences in the two captive provisions are in practice. The controlling authority in each case seems to be the DOD Manual.

As noted above in the discussion of Section 2.1, there is certainly an intuitive appeal to the idea that, if a U.S. person is taken hostage abroad, the IC will attempt to locate the person and collect SIGINT in aid of recovery. But the precise legal theory for the collection is not as clear. There appear to be two likely possibilities.

First, SIGINT collection might be justified under the Fourth Amendment with the implied consent of the hostage. Many hostages, but perhaps not all, probably would consent to SIGINT collection designed to aid their rescue, recovery, or escape. But it is not at all clear that the mere fact of being taken hostage is enough to establish valid consent, which may be tacit but usually must be specific. See *Florida v. Jimeno*, 500 U.S. 248, 251-252 (1991); *Schneckloth v. Bustamonte*, 412 U.S. 218, 227 (1973); *Lopez v. United States*, 373 U.S. 427 (1963); *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990).

Second, exigent circumstances would also justify collection in at least some cases of hostage-taking abroad. See generally *Mincey v. Arizona*, 437 U.S. 385 (1978); *Michigan v. Fisher*, 558 U.S. 45 (2009). In domestic settings, the courts have permitted exigent-circumstances searches to look for hostages. See, e.g., *United States v. Cooks*, 920 F.3d 735 (11th Cir. 2019). The new limits in the SIGINT Annex on collection targeting U.S. person hostages (SA § 2.5.c.(2)(1)(1)-(5)) may suggest a relatively greater reliance on exigency rather than consent.

To the extent that they are valid under the Fourth Amendment, either of these theories – consent or exigency – also would remove the collection from Section 2.5 of Executive Order 12333 and FAA § 704, which apply only where a warrant would be required if the SIGINT collection were undertaken for law enforcement purposes. Without explaining why, the

September 2020 Trump Memorandum on hostages (cited in the discussion of SA § 2.1 above) expressly provides that "[w]ith regard to such collection directed against United States persons held captive abroad, the IC may do so without obtaining, pursuant to section 2.5 of Executive Order 12333, approval from the Attorney General or his determination that the technique is directed against a foreign power or an agent of a foreign power."

This language in the Trump Memorandum may reflect reliance on consent or exigency, rather than any more radical possibility. For completeness, however, the more radical possibilities include (1) an implicit amendment of Section 2.5, authorizing collection in hostage situations without regard to whether the U.S. person is an agent of a foreign power, cf. 24 Op. OLC 29 (2000); or (2) a conclusion that hostage-related SIGINT collection is exempt from Section 2.5 because it is not undertaken for "intelligence purposes," despite the breadth of the terms "intelligence" and "intelligence activities" as defined in Section 3.5(a) and (e)-(g) of the Executive Order. A third, less radical possibility is also worth mentioning: in some hostage situations, it may be possible to collect SIGINT on a theory that the non-U.S. person captor, rather than the U.S. person captive, is the only real target (e.g., because the captor controls and is using the captive's devices and accounts). But that may not be the case in all situations. The Trump Memorandum refers expressly to collection being "directed against" the U.S. person hostage – this is not necessarily the same as targeting, because "directed against" might be understood to refer to facilities at which collection is directed, such as the U.S. person's mobile phone. But the SIGINT Annex is very clear in referring to "intentional targeting of a U.S. person captive" (§ 2.5.c.(2)(a)). In any event, whatever its relationship to Section 2.5 of Executive Order 12333, the Trump Memorandum does not address or suggest any retreat from or challenge to FAA § 704 (50 U.S.C. § 1881c)), which provides that "[n]o element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes," except as authorized in the statute.

(d) Limitations on Collection Targeting Non-U.S. Persons in the United States. Section 2.5.d of the Annex allows the USSS to "target a non-U.S. person in the United States only if the collection is not governed by FISA" and if one or more of several additional circumstances exists. The approach here is very similar to the approach described above for collection targeting a U.S. person: there is a baseline requirement that the collection be outside the scope of FISA and then a set of additional circumstances that describe several specific ways of ensuring that that is the case or impose requirements that are somewhat analogous to those in FISA. The additional circumstances are as follows:

(1) Consent. Here, as with the analogous provision for U.S. persons, consent tends to bring collection out from under the regulation of FISA (and the Fourth Amendment).

(2) A redacted circumstance. This circumstance is redacted, but it provides that the USSS may target a non-U.S. person located in the U.S. "for the purpose of acquiring significant

foreign intelligence or counterintelligence" under certain specified conditions: (a) the target is something redacted; (b) DIRNSA or a delegee approves the collection; and (c) the collection is limited to communications that have at least one end abroad at the time of acquisition (or, when the communications are domestic at the time of acquisition, the Attorney General approves the collection). This must be a narrow provision, to the extent that it applies outside of FISA but still purports to cover domestic as well as international communications (albeit with Attorney General approval). For example, in 1978, the Department of Justice advised Congress that "foreign states and their official agents, to the extent that they are not subject to our laws, are not protected by the Fourth Amendment," such that collection targeting them would not require a warrant or qualify as "electronic surveillance" under FISA, but the statute's legislative history explains that Congress did not intend this to exempt surveillance of such persons from FISA, and rather "intended to exclude only those surveillances which would not require a warrant even if a U.S. citizen were the target." HPSCI 1978 FISA Report at 64, 69 n.34. The exemption in the SIGINT Annex is difficult to understand due to redactions.

(3) Another redacted circumstance involves a business entity controlled by a foreign government. This appears to involve targeting something (perhaps a specific type of communications facility or channel, or specific communications) of foreign powers in the United States as defined in 50 U.S.C. § 1801(a)(1)-(3) and the equivalent language in Annex § G.2. Such foreign powers may be targeted under FISA for one year, which is longer than other FISA targets, see 50 U.S.C. § 1805(d)(1), and the Annex also allows such targeting for one year with certain findings from the Attorney General when there is a foreign intelligence or counterintelligence purpose. Again, there are only very limited circumstances in which collection of this sort would be outside the scope of FISA, but the Annex appears to impose limits that are analogous in certain ways to those in FISA.

(4) The fourth circumstance involves targeting a non-U.S. person inside the United States when the Attorney General finds probable cause that he is an agent of a foreign power and there is a purpose to acquire significant foreign intelligence or counterintelligence. This applies, again, only to collection scenarios, described above, that do not qualify as "electronic surveillance" or a "physical search" under FISA.

(5) The final circumstance applies to so-called "roamers" under FAA § 702, and is analogous to 50 U.S.C. § 1805(f). Cf. Prior Annex § 4.A.1.(d)(2) (page A-6). Under Section 1805(f), a non-U.S. person target under FAA § 702 who appears in the United States – and therefore ordinarily would no longer be eligible for targeting – may nonetheless be subject to continued collection for up to 72 hours in certain circumstances even without an emergency authorization under traditional FISA, 50 U.S.C. §§ 1805(e), 1824(e). The SIGINT Annex sets up a similar system for collection that is not "electronic surveillance" or a "physical search" under FISA. Collection is limited to 72 hours and may continue only if another provision of the Annex (or FISA) can be satisfied.

In one respect, the Annex is slightly broader than Section 1805: the statute applies only when "a lapse in the targeting of [the roamer] person poses a threat of death or serious bodily

harm to any person," while the SIGINT Annex applies also where there is a threat of "destruction of, or significant damage to, property" or the "failure to obtain significant foreign intelligence or counterintelligence, or a delay in obtaining such information, that would result in substantial harm to national security." SA § 2.5.d.(5)(a)2.a.(ii) and b. On the other hand, while the statute allows continued collection on roamers for 72 hours based on determinations made by the head of an IC element with notice to the Attorney General, 50 U.S.C. § 1805(f)(1)(B), the SIGINT Annex appears to require AG approval unless it is not practicable to obtain. The statutory provision, and the Annex, have interesting implications for the question whether FAA § 702 collection may be broader than "electronic surveillance" and "physical searches" as defined by traditional FISA.

Exceptions. Finally, after setting out an elaborate scheme of considerations, prohibitions, and limitations for SIGINT collection, Section 2.6 of the Annex purports to identify a separate category of exceptions to certain of the limits in Section 2. It is not clear why these exceptions could not be built directly into the Annex's main categories, but they do cover the same subject matter as certain legacy documents that in some cases were separate from the Prior Annex.

The first exception is for "Counterdrug Activities and Activities to Counter Transnational Organized Crime." Notwithstanding the limitations on surveys and targeting U.S. persons in §§ 2.5.a. and b., the USSS may target "U.S. persons outside the United States who are suspected of involvement in international narcotics trafficking or transnational organized crime." This is consistent with Section 2.6 of Executive Oder 12333 and 50 U.S.C.A. § 3039(a), and it has roots in Appendix A to the Prior Annex and Annex J to USSID-18. The exception to the limitations – i.e., the permitted collection – "only applies where the communicants do not have a reasonable expectation of privacy in such radio communications and the communications are not otherwise protected by the Fourth Amendment." SA § 2.6.a. As such, the collection should not be regulated by Section 2.5 of Executive Order 12333 or by FAA § 704 (50 U.S.C. § 1881c), both of which apply only to collection that raises issues under the Fourth Amendment.

The second exception is for "Illicit Communications," SA § 2.6.b., and applies notwithstanding the prohibition on collecting domestic communications in SA § 2.4.a, and the limitations on collection in SA § 2.5. This exception has roots in USSID-18 Annex F and in pages A-2 to A-3 and A-11 of the Prior Annex. Annex F to USSID-18 explains that "'illicit communications' means a communication transmitted in violation of either the Communications Act of 1934 and regulations issued thereunder or international agreements, which because of its explicit content, message characteristics, or method of transmission, is reasonably believed to be a communication to or from an agent or agents of foreign powers, whether or not U.S. persons." Collection is permitted for a period not to exceed 90 days, where there is a purpose of acquiring significant foreign intelligence or counterintelligence and the Attorney General approves the collection based on his finding that the communications violate the Communications Act of 1934 and based on the message attributes the messages are to or from foreign powers or agents of foreign powers.

*. *. *

Despite its various considerations, prohibitions, and limitations on SIGINT activity, the Annex recognizes (§ 2.2.b) that it is "possible that the USSS may incidentally collect domestic communications and communications to, from, or about U.S. persons in the course of authorized collection of foreign communications." As defined in the Annex, "incidental" collection includes not only inevitable and expected collection (e.g., of a surveillance target's interlocutors), but also appears to include genuinely undesired collection that happens by accident (e.g., through misidentification of a target or a change in target status that affects the legality of collection). See SA § G.2 (definition of "incidental collection of communications"). That does not pose any kind of problem, but it is worth noting that some commentators refer to the former as "incidental" and to the latter as "unintentional" or "inadvertent." See, e.g., *Hasbajrami*, 945 F.3d at 646; compare 50 U.S.C. § 1806(i) (unintentional) with 50 U.S.C. § 1813 (incidental). The Annex's rules for retention and dissemination of information, discussed below, deal with such information. See, e.g., SA § 4.6.b. Regardless of how it is labeled, of course, a targeting or collection violation would still be a violation under the SIGINT Annex.

3. PROCESSING AND QUERYING

Once SIGINT has been collected, it may need to be processed into an intelligible or useable form, and it can be queried. Section 3 of the SIGINT Annex governs these activities, the next stage after collection in the intelligence lifecycle. Technically, Section 3 "governs processing of SIGINT and establishes requirements for querying unevaluated SIGINT in addition to the requirements" for such activities in Sections 3.3.f.(1) and 3.3.g.(2) of the DOD Manual. SA § 3.1. By "unevaluated," the Annex means "SIGINT that has not been determined to qualify for retention," SA § G.2, which is analogous to "unminimized" information under FISA, or "raw" intelligence. The two cross-referenced elements of the DOD Manual provide protections for U.S. person information (USPI), which is information that could identify a U.S. person, such as a name. Among those protections are a requirement to limit access to USPI, to use queries that are relevant to an appropriate intelligence mission (e.g., not to search for LOVEINT), to tailor queries, and to document queries so that they can be audited.

Processing is the main step between collection and analysis, and so the Annex provides that the "USSS may process SIGINT to prepare data for analysis." SA § 3.2. Once collected (e.g., from a forward-deployed sensor or other remote location), data may be "forwarded to NSA or to intermediate processing facilities" where appropriate capabilities exist to handle large quantities of data. Cf. Prior Annex § 4.A.3.(a)(2) (page A-9).

It is important to understand the intersection of data processing, bulk data collection, and surveys as discussed above. As previously noted, PPD-28 generally prohibits SIGINT collection in bulk (subject to six important exceptions), but even the general prohibition is subject to a caveat that has to do with processing. Under Section 2, footnote 5 of PPD-28, "[t]he limitations contained in this section [concerning bulk collection] do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection." In other words, if NSA needs to "acquire" or "collect" a large volume of communications or other data in order to

process the data using selection terms, and if NSA then promptly discards the data that are not responsive to the selection terms, it is not considered a collection in bulk. NSA's PPD-28 Section 4 Procedures (page 7, footnote 2) make an explicit application of this rule to "search and development activities permitted by Paragraph El.2.a. of Annex E of USSID SP0018 or the processing of a signal that is necessary to select specific communications for forwarding for intelligence analysis." A "search and development" activity under Annex E of USSID-18 is the ancestor of a "survey" under Section 2.5.a(2) of the SIGINT Annex. It is not clear how long temporary-retention-in-aid-of-processing may endure without qualifying as "retention," but it is clear from the PPD-28 Section 4 procedures that it may not extend to the point of permitting analysis of the information. As noted above, certain surveys must not exceed two hours without special approval, SA § 2.5.a.2.(c)(1)-(2), and it is likely that temporary retention is similarly measured in hours (or perhaps a small number of days) rather than longer increments. Cf. Prior Annex § 4.A.3.(a)(2).

It is not clear whether PPD-28's approach to bulk collection also applies to the SIGINT Annex. The Annex cross-references the definition of "collection" in the DOD Manual, see SA § G.2, and the DOD Manual provides that "[i]nformation is collected when it is received by a Defense Intelligence Component, whether or not it is retained by the Component for intelligence or other purposes," but does "not include … [i]nformation that only momentarily passes through a computer system of the Component" or "[i]nformation on the Internet or in an electronic forum or repository outside the Component that is simply viewed or accessed by a Component employee but is not copied, saved, supplemented, or used in some manner." DOD Manual § G.2. This would exempt immediate processing of the sort that occurs with a packet-sniffer (in which information is retained in active memory "momentarily" and then discarded if not responsive to the programmed collection criteria), but it does not seem to go as far as PPD-28 in exempting from "collection" information that is discarded after prompt (but not momentary) post-acquisition processing.

Processing is important not only in reducing the volume of collected information, but in preparing collected information for querying and analysis. Section 3.2.a. of the SIGINT Annex provides several examples of ways in which collected information may be processed:

> (1) Processing information to characterize or understand signals and communications.
>
> (2) Taking all steps necessary to convert information into an intelligible form intended for human inspection, including decryption or cryptanalysis.
>
> (3) Reverse engineering malicious signals or potential malware.
>
> (4) Combining SIGINT information with other information to facilitate activities such as data correlation, retrieval, formatting, and conversion.
>
> (5) Identifying or labeling information for more efficient analysis.

(6) Processing information to limit USPI and non-pertinent information as set out in Paragraph 2.3.

Accordingly, for example, processing might include converting the format of data (e.g., from analog or other forms to digital), removing encryption, isolating and disabling malware, combining multiple collected sets of data to establish connections between them, tagging data, and filtering out USPI and non-pertinent information. The basic purpose of processing, and the net effect of these processing steps, is to render the collected data more useful for exploitation through querying or other analysis.

Section 3.3 of the SIGINT Annex regulates queries of collected and processed information. As noted above (Part II.A), the querying rules are among the most significant changes from the Prior Annex, reflecting both the growing importance of querying and the growing policy focus on querying. The focus on querying may also reflect technological advancements since the Prior Annex was last significantly updated in 1988: paper, magnetic tape, microfilm, and other analog data sets are not nearly as amenable to automated querying and other exploitation as digital data. In the old days, querying was much more a question of a human being looking through a data set for the desired information.

Given that, it is notable that neither the SIGINT Annex nor the DOD Manual defines the term "query." Cf. DOD Manual § 3.3.f.(1). As defined by Congress in the FISA Amendments Act, a query "means the use of one or more terms to retrieve the unminimized [unevaluated] contents or noncontents located in electronic and data storage systems." 50 U.S.C. § 1881a(f)(3)(B). As a practical matter, that is likely pretty close to the definition that is (implicitly) in use in the SIGINT Annex: by its nature, a query must involve terms that are used to select and retrieve information from storage. However, there is also no explicit requirement that the "terms" used in queries meet the definition of "selection term" in the Annex, which means that there is no explicit requirement that the terms used in a query "limit[], to the greatest extent practicable, the scope of information sought, consistent with the purpose of the collection or query." SA § G.2; cf. SA § 2.2.a.(2) (requiring "targeted collection using selection terms whenever practicable"). On the other hand, Section 3.3.f.(1)(b) of the DOD Manual requires all DOD elements, when "retrieving information electronically," to "[t]ailor queries or other techniques to the greatest extent practicable to minimize the amount of USPI returned that is not pertinent to the intelligence mission and purpose for the query."

Under the SIGINT Annex (§ 3.3), queries may be conducted for the same three purposes as collection under SA § 2.1 as discussed above: "foreign intelligence, counterintelligence, and support to military operations purposes, and for the purpose of protecting the safety or enabling the recovery of a U.S. person reasonably believed to be held captive outside the United States by a foreign power or other non-U.S. person." Queries retrieve stored data from a repository in ways that are similar to how selection terms capture data moving through a communications channel, see SA § 3.3, and the Annex imposes rules that treat queries somewhat like independent collection events. Unlike the Prior Annex, however, the new SIGINT Annex spells out those requirements with greater particularity and subjects them to separate

requirements. This is notable because there is a growing body of caselaw on the extent to which rules governing querying (and other post-acquisition use and treatment of data) affect a single, holistic assessment of the "reasonableness" of SIGINT activity under the Fourth Amendment, or whether querying (and other post-acquisition activities) should be treated as discrete Fourth Amendment events in and of themselves. Whether assessed under the holistic approach or the discrete approach, there is also a growing focus on the legal and policy standards that ought to govern querying and related activities. See, e.g., NSIP § 17:11 at 717; *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019) (upholding incidental collection, and discussing unintentional collection and querying, under FAA § 702).

Under the SIGINT Annex, queries in two categories are given special attention. First, there are queries that are "reasonably likely" to return USPI; second, there are queries that are affirmatively designed to retrieve USPI. As to the former, queries "using selection terms that are reasonably likely to result in, or have resulted in, the retrieval of communications to, from, or about a U.S. person" must be "designed" so that they "defeat, to the extent practicable under the circumstances, the retrieval of those communications, or data related to such communications, not relevant to the purposes specified above" for permitted queries. SA § 3.3. In other words, these queries must try to reduce the incidental return of non-pertinent USPI. As noted above, a similar (partially redacted) standard applies to the use of selection terms in collection under SA § 2.5.a.(1).

Queries that are affirmatively intended to retrieve international communications to, from, or about a U.S. person, or a person located in the United States, may only be used in one or more of seven defined circumstances set out in Section 3.4 of the Annex:

a. With appropriate consent. The analogous provision in the Prior Annex is Section 4.A.1.(a)(1) (page A-5).

b. If the person is a current FISA target (including under FAA § 704, but not under FAA § 702). The analogous provisions in the Prior Annex are Sections 4.A.1.(a)(2) and (4) (pages A-5 and A-6); it appears that there is no longer any general requirement to consult with the Attorney General before proceeding on this basis, even with respect to FBI FISA targets.

c. In a redacted circumstance that has to do with "cyber threat activity of foreign actors." This appears to be new, and potentially significant, but redactions make it difficult to comment further.

d. In another redacted circumstance having something to do with a relationship between the subject of the query and something pertaining to a "foreign power in the United States." Redactions inhibit meaningful comparisons and commentary here as well. Cf. Prior Annex § 4.A.1.(b) (also redacted) (page A-6).

e. For 72 hours when a non-U.S. person FAA § 702 or other targeted roamer enters the United States. The analogous provision in the Prior Annex, governing collection, appears to be Section 4.A.1.(d)(2) (page A-6). Cf. 50 U.S.C. § 1805(f).

f. With the approval of DIRNSA (or, in all but one case, a delegee) in several circumstances:

(1) To protect the safety or enable the recovery of the U.S. person who is the subject of the query if the U.S. person is being held captive abroad by a non-U.S. person or entity, with "prompt" notice to the Department of Justice. As discussed above concerning SA §§ 2.1 and 2.5.c, the analogous provision in the Prior Annex is Section 4.A.1.(a)(3) (page A-5).

(2) For up to 72 hours in exigent circumstances similar to those defined in DOD Manual § 3.5(h) and discussed above. The analogous provision in the Prior Annex is Section 4.A.1.(d)(1) (page A-6). Querying for longer than 72 hours may be permitted with Attorney General approval under SA § 3.4.(g)(2), discussed below.

(3) Where the subject of the query is a non-U.S. person located in the United States, but the query is limited to communications obtained at a time when the person was reasonably believed to be abroad (cf. 50 U.S.C. § 1881a(b)(4)), or if the subject of the query has a redacted relationship with a governmental foreign power. This appears to be a new provision, but the redaction makes it difficult to be sure.

(4) With DIRNSA's approval (not a delegee's approval) for queries of particular foreign power datasets that seek information about (not to or from) a person under certain conditions. Those conditions are that there is "specific information" indicating that the person "is the target or possible agent of a foreign power," which seems to mean that the U.S. person could be "targeted" by the foreign power for recruitment as an intelligence asset or perhaps in other ways; that the query is designed to retrieve "significant" information; and that there is a "high likelihood" that any USPI in the dataset will have intelligence value. To illustrate the gist of this with a hypothetical example, if NSA gains access to a foreign intelligence agency's internal communications concerning U.S. government officials who should be blackmailed or killed, or have been recruited to do something for the foreign intelligence agency, it may be appropriate to query that database. This appears to be new. In theory, querying here could result in a reduction of disseminated information, because the entire foreign dataset probably would be subject to dissemination as "foreign intelligence," and queries might result in dissemination only of relevant portions of the dataset.

g. With the approval of the Attorney General, for a period not to exceed 90 days, where the queries are designed to retrieve international communications to, from, or about a U.S. person or a person in the United States, in several circumstances:

(1) Where there is probable cause that the person is an agent, officer, or employee of a foreign power (the FAA § 704 collection standard) and the purpose of the query is to acquire

significant foreign intelligence or counterintelligence. This applies to persons who are not current FISA targets (but likely could be) and is analogous to Section 4.A.1.(a)(4) (page A-6) of the Prior Annex.

(2) Various situations involving serious threats in which the person is either a potential victim or perpetrator of the threatened harm. This is related to SA § 3.4.f.(2) discussed above but is not limited to 72 hours. Moreover, it applies more broadly, including in cases where the U.S. person is not an agent of a foreign power but "is reasonably believed to have a foreign connection," a term defined in the DOD Manual to require "[a] reasonable belief that the U.S. person is or has been in contact with, or has attempted to contact, a foreign person or a representative or agent of a foreign country, for purposes harmful to the national security interests of the United States; or when a reasonable belief exists that the U.S. person is acting or encouraging others to act in furtherance of the goals or objectives of a foreign person or power, or a representative or agent of a foreign power, for purposes harmful to the national security interests of the United States."

(3) In the same conditions as above in SA § 3.4.f.(4) for queries of particular foreign data sets with DIRNSA's approval, except that the queries may be designed to retrieve communications to or from, as well as about, the person who is the subject of the query.

Taken together, these authorized circumstances permit U.S. person queries in a way that is more precisely defined (more prescriptive), and also broader, than what was permitted under the Prior Annex, which focused on standards requiring the U.S. person to be an agent of a foreign power. The SIGINT Annex therefore moves some of the way, but not all of the way, towards permitting querying for any legitimate foreign intelligence or related purpose. It is difficult to be sure exactly how far it goes due to redactions, but while the Annex recognizes some circumstances in which the U.S. person will be an agent of a foreign power – e.g., when he or she is a FISA target – it also clearly recognizes several other circumstances. It presumably reflects a conclusion that the Fourth Amendment permits querying in all of the specified circumstances, including as to information collected solely under the authority of the SIGINT Annex itself (e.g., not under statutory standards or with judicial approval based on a finding of probable cause). The Annex does not suggest that collection, as opposed to querying, would be permitted under the Fourth Amendment in all of the circumstances specified in Section 3.4. Cf. *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019). There are also more significant statutory restrictions on collection as opposed to querying.

Finally, Section 3.5 of the SIGINT Annex provides that the limitations on queries discussed above do not apply to "communications metadata analysis, including contact chaining," when done for one of the three permitted purposes for collection in SA § 2.1. In such cases, the normal querying rules in SA §§ 3.3 and 3.4 do not apply and the metadata analysis and contact chaining may proceed "without regard to the physical location or nationality of any of the communicants or the location or registration of any device." Although the USA Freedom Act put an end to bulk collection under FISA's pen register and business records provisions, and National Security Letters, bulk SIGINT collection remains permitted in the six categories

described in PDD-28. This exception carries forward a version of the 2008 Special Procedures Governing Communications Metadata Analysis (SPCMA) that were adopted as a supplement to the Prior Annex.

4. RETENTON

After collection and processing, the next stage in the intelligence lifecycle is retention. In keeping with Sections 2.3 and 2.4 of Executive Order 12333, and Procedure 3 of the DOD Manual, the retention standards in the SIGINT Annex are focused on USPI. Section 4.1 of the Annex explains that it does two things. First, it "modifies retention periods for SIGINT information to the extent that the retention periods conflict with Paragraphs 3.3.c and 3.3.e" of the DOD Manual. This might appear to be impossible in light of the hierarchical relationship between the two documents, but Section 3.3.i of the DOD Manual provides that "[a]ny retention of USPI obtained from SIGINT is subject to the procedures in the classified annex to this issuance and any applicable Presidential directives," and the SIGINT Annex apparently treats this as a general authorization to depart from the Manual with respect to SIGINT retention. Both the DOD Manual and the SIGINT Annex were authorized by the same senior officials, and they (or their advisors) presumably understood what they were approving.

Second, the Annex also "implements" 50 U.S.C. § 1813, a law enacted in 2014 that (to my knowledge) is the first direct Congressional regulation of SIGINT retention outside the ambit of FISA (the DOD Manual is also designed in part to implement Section 1813). Section 1813 applies to "any nonpublic telephone or electronic communication acquired without the consent of a person who is a party to the communication, including communications in electronic storage." 50 U.S.C. § 1813(a)(1). Intelligence element heads are required by the statute to adopt procedures to deal with such communications when they are "reasonably anticipated" to be acquired as part of an "intelligence collection activity" that is conducted without a court order, subpoena, "or similar legal process." 50 U.S.C. § 1813(b)(3)(A). In essence, therefore, Section 1813 applies to SIGINT conducted under Executive Order 12333 and the SIGINT Annex.

The procedures required under Section 1813 must generally prohibit retention of covered communications in excess of five years subject to several enumerated exceptions. Many of these exceptions are unremarkable, such as the one for communications "affirmatively determined, in whole or in part, to constitute foreign intelligence or counterintelligence or [to be] necessary to understand or assess foreign intelligence or counterintelligence." 50 U.S.C. § 1813(b)(3)(B)(i). A catch-all exception applies where "retention for a period in excess of 5 years is approved by the head of the element of the intelligence community responsible for such retention, based on a determination that retention is necessary to protect the national security of the United States, in which case the head of such element shall provide to the congressional intelligence committees a written certification." 50 U.S.C. § 1813(b)(3)(B)(vii). That certification must describe all of the following: "(I) the reasons extended retention is necessary to protect the national security of the United States; (II) the duration for which the head of the element is authorizing retention; (III) the particular information to be retained; and (IV) the measures the

element of the intelligence community is taking to protect the privacy interests of United States persons or persons located inside the United States." 50 U.S.C. § 1813(b)(3)(B)(vii)(I)-(IV).

In keeping with Section 1813, neither the Annex nor the DOD Manual applies to "the retention of information obtained under FISA, which has its own [retention] provisions." DOD Manual § 3.3.a; see SA § 1.2.b. In particular, FISA prescribes "minimization procedures" that govern retention of information and that are adopted by the government and reviewed by the FISA Court under 50 U.S.C. §§ 1801(h) and 1805(a)(3) for electronic surveillance, under 50 U.S.C. §§ 1821(4) and 1824(a)(3) for physical searches, under 50 U.S.C. §§ 1861(c)(1) and (g) (sunset) for tangible things orders, under 50 U.S.C. §§ 1881a(e) and (j)(2)(C) for FAA § 702 collection, under 50 U.S.C. §§ 1881b(b)(1)(D) and (c)(3(C) for FAA § 703 collection, and under 50 U.S.C. §§ 1881c(c)(B)(4) and (c)(1)(C) for FAA § 704 collection (the FAA § 704 minimization procedures are reviewed by FISA Court only as to their dissemination provisions). Under 50 U.S.C. §§ 1842(h) and 1843(d), for FISA pen register surveillance, the Attorney General must adopt "privacy procedures" that govern retention of information, but the procedures are not reviewed or approved by the FISA Court.

Outside the scope of FISA, under Section 4.2 of the Annex, the USSS generally "may retain unevaluated SIGNT for up to 5 years from the time it is collected." This is consistent with DOD Manual § 3.3.c.(1) and particularly with 50 U.S.C. § 1813. If the information is enciphered or reasonably believed to have secret meaning, it may be retained "for sufficient duration to permit exploitation." SA § 4.2. This appears to follow from DOD Manual § 3.3.c.(6), which provides that the relevant time limits begin only when collected "information is processed into intelligible form." Similarly, under FISA, "where communications are encoded or otherwise not processed, so that the contents of the communication are unknown, there is no requirement to minimize … until their contents are known." HPSCI 1978 FISA Report at 57.

Section 4.3 of the Annex authorizes DIRNSA (with a certification to the Congressional Intelligence Committees) to approve "the retention of unevaluated SIGINT for up to an additional 20 years beyond the default retention period." This appears to implement the catch-all exception in 50 U.S.C. § 1813, as discussed above. 50 U.S.C. § 1813(B)(3)(B)(vii). Under DOD Manual § 3.3.c.(2)(B), information collected by targeting non-U.S. persons outside the United States, including incidentally collected USPI, may be retained for 25 years. But certain other categories of information may be retained only for an additional five years under DOD Manual § 3.3.c.(5).

Section 4.4 of the SIGINT Annex allows potentially indefinite retention of several categories of evaluated SIGINT which correspond to the categories specified in 50 U.S.C § 1813.

The first category involves information that poses no real threat to U.S. persons' privacy interests. It consists of "foreign communications [i.e., communications with at least one end outside the U.S.] that are determined to constitute, in whole or in part, foreign intelligence or counterintelligence, or information necessary to understand or assess foreign intelligence or counterintelligence, and in which all parties to the communication are reasonably believed to

be non-U.S. persons, and from which any USPI has been removed." SA § 4.4.a. Retention here may be permanent. This reflects the basic idea that retention standards for SIGINT are focused on protecting U.S. persons, and the importance of retaining pertinent intelligence information. The exception applies only to communications that have been determined to be pertinent (cf. 50 U.S.C. § 1813(b)(3)(B)(i)), and is more protective of foreign persons' privacy interests than 50 U.S.C. § 1813(b)(3)(B)(iv). The Annex does require the USSS to take steps to destroy certain non-pertinent communications of certain non-U.S. persons in partially redacted circumstances. SA § 4.6.c.

International communications "to, from, or about a U.S. person" may also be retained beyond five years in four other situations based in part on 50 U.S.C. § 1813. SA § 4.4.b.(1)-(4). First, if the information "has been affirmatively determined, in whole or in part, to constitute foreign intelligence or counterintelligence, or information necessary to understand or assess foreign intelligence or counterintelligence." As noted in the previous paragraph, this is not surprising, and analogous to other minimization rules that allow long-term retention of pertinent information after it has been reviewed. For example, such information often makes its ways into intelligence reports that are disseminated within the government and do not automatically age off. See 50 U.S.C. § 1813(b)(3)(B)(i).

Second, information that may not have direct intelligence value but is necessary for cryptanalysis or related functions may also be retained, albeit with USPI subject to masking unless it is essential to the purpose for which the information is retained. This reflects the fact, discussed above, that cryptanalysis may benefit from relatively large data sets, including data sets that can be used to train artificial intelligence models or the like. It appears to be based on 50 U.S.C. § 1813(b)(1)(B)(i) and/or (iii).

Third, a "communication necessary to protect against an imminent threat to human life may be retained in excess of 5 years" if reported to the Congressional Intelligence Committees. If the threat is indeed imminent, retention beyond five years may not be directly useful, but it could be relevant to identifying targets of long-term interest to terrorists or other adversaries. In any event, the requirement appears to be based on 50 U.S.C. § 1813(b)(3)(B)(v).

Fourth and finally, information needed for technical assurance or compliance may be retained for longer than five years. This is in keeping with SA § 1.3.f, as discussed above, and with 50 U.S.C. § 1813(b)(3)(B)(vi).

Section 4.5 of the Annex includes an exception for communications metadata, including the results of contact chaining and other analysis of metadata, that is analogous to the exception for metadata analysis in Section 3.5.

Under Section 4.6.a. of the SIGINT Annex, the USSS generally may not retain domestic communications in which a person has a reasonable expectation of privacy and as to which warrant would be required to collect for law enforcement purposes. The only exception applies where the Attorney General determines that retention is lawful and the contents indicate a

threat of death or serious bodily harm to a person. Cf. 50 U.S.C. § 1813(b)(3)(B)(v); 1806(i) ("In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.").

Under Section 4.6.b., the USSS will generally "destroy promptly upon recognition" any communication collected as a result of "inadvertent targeting of a non-consenting U.S. person." As noted above, the Annex uses the word "incidental" to mean the "collection of the communications of a person whose communications are not deliberately sought but are nonetheless collected. Such collection is considered incidental regardless of whether it is expected or reasonably anticipated to occur." SA § G.2. Here, by using the word "inadvertent," the Annex seems to mean a sub-set of such "incidental" collection, in which the collection is both unexpected and undesired, but happens by accident, unintentionally. Destruction is not required if retention is permitted by FISA (perhaps this would be the case if the U.S. person were, by coincidence or otherwise, a FISA target), is otherwise consistent with Sections 4.2-4.5 of the Annex, and the communications contain evidence of a crime, significant foreign intelligence or counterintelligence, or information indicating a threat of serious harm to life or property. Under Section 5.4.b. of USSID-18, inadvertently collected communications solely between U.S. persons are also generally to be destroyed upon recognition.

Section 4.6.c. imposes a similar destruction requirement for communications acquired as a result of inadvertent targeting of certain non-consenting non-U.S. persons who are in the United States at the time of the collection. Redactions make it difficult to know exactly who and what is protected by this provision.

5. DISSEMINATION

The final stage of the intelligence lifecycle is dissemination. Section 3.4 of the DOD Manual governs dissemination of USPI collected or retained by all Defense Intelligence Components, but also provides that it "does not apply to the dissemination of information … disseminated pursuant to other procedures approved by the Attorney General." DOD Manual § 3.4.a. The SIGINT Annex was approved by the Attorney General, and therefore might be seen as supplanting the dissemination provisions in the DOD Manual, but the Annex provides explicitly in Section 5.1 that the "dissemination of USPI and information derived from SIGINT must also comply with the requirements of Procedures 4 and 5 [Sections 3.4 and 3.5] of" the DOD Manual.

The dissemination rules in the SIGINT Annex, Section 5.2, are generally consistent with similar rules in minimization procedures under FISA and other authorities. In traditional FISA and the FAA, minimization procedures must "prohibit the dissemination … of nonpublicly available information concerning unconsenting United States persons consistent with the need

of the United States to obtain, produce, and disseminate" foreign intelligence information, 50 U.S.C. §§ 1801(h)(1), 1821(4)(A), 1881a(e), 1881c(c)(b)(4), and must also "require that nonpublicly available information, which is not [protective foreign intelligence information as defined in 50 U.S.C. § 1801(e)(1)] shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance." 50 U.S.C. §§ 1801(h)(2), 1821(4)(B). Under ODNI standards, "[i]n general, for non-public information concerning an unconsenting U.S. person, agencies may only include the identity of the U.S. person if it itself constitutes foreign intelligence, is necessary for the recipient to understand the foreign intelligence being transmitted, or is evidence of a crime." ODNI, Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act at 2 (Nov. 2017).

The SIGINT Annex is broadly consistent with the FISA rules for dissemination. It generally forbids the inclusion of USPI in a SIGINT dissemination unless the recipient is reasonably believed to have a need for the USPI for the performance of its lawful missions or functions and one or more of certain other conditions are met. Those conditions are (a) proper consent; (b) the USPI is publicly available; (c) the "USPI is necessary for the intended recipients to understand the foreign intelligence or counterintelligence information to which the USPI pertains or to assess its importance"; (d) the USPI is evidence of a crime that is being disseminated for law enforcement purposes and is reported to the Department of Justice, cf. 50 U.S.C. § 1801(h)(3); (e) the USPI is disseminated to protect the safety or enable the recovery of a U.S. person captive held abroad by non-U.S. persons; or (f) the dissemination is otherwise required by law or directive.

The Annex provides six examples of situations in which USPI would be properly disseminated under (c), on the theory that it is necessary to understand or assess intelligence or counterintelligence. Many of the examples are straightforward, such as where the information "indicates that the U.S. person may be a foreign power, an agent of a foreign power, or an officer or employee of a foreign power." SA § 5.2.c.(1).

The final example is a situation, not unknown to history, in which the intelligence "indicates that the U.S. person is a senior official of the Executive Branch of the U.S. Government." In such a case, the SIGINT Annex provides (SA § 5.2.c.(6)), "only the official's title" – e.g., National Security Advisor – "will be disseminated," and DIRNSA or a delegee must "ensure that domestic political or personal information that is not necessary to understand foreign intelligence or counterintelligence or assess its importance is not disseminated." This is similar to the standard in Section 4.A.4.(c) of the Prior Annex (page A-10). Cf. ICD 112, Annex A (2017) (Gates Procedures for disseminating identities of Members of Congress).

A similar approach is required under FISA. In general, under FISA, "all minimization procedures [must] contain a requirement that any information acquired which is not [protective] foreign intelligence information … not be disseminated in a manner which identifies an individual United States person, without his consent, unless the identity is necessary to understand foreign intelligence information or to assess its importance." HPSCI

1978 FISA Report at 61; see 50 U.S.C. § 1801(h)(2). But the legislative history recognizes that "sometimes it might be difficult or impossible to make sense out of the information without a U.S. person's identity":

> One example would be the identity of a person who is the incumbent of an office of the executive branch of the U.S. Government having significant responsibility for the conduct of U.S. defense or foreign policy, such as the Secretary of State or the State Department country desk officer. The identities of such persons would frequently satisfy the "necessary to understand" requirement, especially when such person is referred to in the communications of foreign officials. This example does not mean, however, that all the conversations of a particular executive branch official with foreign officials who are under surveillance should be automatically or routinely reported to the U.S. official's superior without his knowledge or consent."

HPSCI 1978 FISA Report at 61; cf. ODNI, *Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act*; ICPG 107.1.

Under Section 5.3 of the Annex, in keeping with the basic purpose of a survey (discussed in SA § 2.5.a), information "necessary for cataloging the constituent elements of the signals environment may be disseminated to the extent that such information is not USPI." The Annex makes clear that survey information that is "[c]ommunications equipment nomenclature" can be disseminated regardless of whether it is USPI. Similarly, under FISA, "trade names such as a Xerox copier, a Boeing 747, etc." are considered to be publicly available and therefore not subject to minimization. HPSCI 1978 FISA Report at 57.

6. POLICY, COMPLIANCE, TRAINING, AND AUDITING

Section 6 of the SIGINT Annex covers various measures "to ensure compliance with the requirements of this annex" and the DOD Manual. Under Section 6.2, DIRNSA "will issue appropriate policies implementing" the SIGINT Annex "in coordination with legal, civil liberties, and privacy officials." As noted above (discussing SA § 1), legislation now requires NSA to have both a Director of Compliance and a Civil Liberties and Privacy Officer. These internal policies are to cover "implementation of the collection, processing, querying, retention, dissemination, and training requirements" in the annex. DIRNSA is also responsible for developing and maintaining compliance programs that address training and auditing, limited access for raw SIGINT, compliance with Annex Sections 2-5, and compliance with relevant portions of the DOD Manual. Personnel with access to raw SIGINT shall receive special training under Section 6.4 of the Annex. Section 6.5 requires auditing and appropriate internal controls for collection, access, queries, retention, and dissemination. The requirements in Section 6 of the SIGINT Annex are more detailed, and hence more transparent, than those in the Prior Annex. They also exist in an environment that is more attuned to privacy and civil liberties. For example, the Privacy and Civil Liberties Oversight Board (PCLOB) has had a significant impact on SIGINT, issuing recommendations for privacy and civil liberties officers in the executive branch, as well as a

series of reports on the USA Freedom Act, PPD-28, FAA § 702, and FISA's business records provisions.

Under Section 6.6 of the Annex, NSA must make certain reports to the Department of Justice and/or other entities. The first report (SA § 6.6.a.(1)) concerns collection, processing, querying, and retention of communications metadata. The complex line between "contents" (as defined in 18 U.S.C. § 2510(8)) and "dialing, routing, addressing, and signaling information" (as set forth in 18 U.S.C. § 3127), and developments in constitutional law including *Carpenter v. United States*, 138 S. Ct. 2206 (2018), make this understandable. Others include a report on the collection method addressed in SA § 2.5.a.(1)(b) and discussed above; a report on failures to comply with SA §§ 2.5, 2.6, or FISA; and certain failures to approve queries as required by SA § 3.4.

7. CERTAIN U.S. PERSON TARGETS OUTSIDE THE UNITED STATES

In the FAA, Congress prescribed a statutory mechanism for intelligence collection targeting U.S. persons reasonably believed to be located abroad. Prior to the FAA, such collection was governed exclusively by Executive Order 12333, principally by Section 2.5, and by constitutional requirements. Under FAA § 704, however, "[n]o element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes, unless a judge of the Foreign Intelligence Surveillance Court has entered an order with respect to such targeted United States person or the Attorney General has authorized an emergency acquisition pursuant to subsection (c) or (d), respectively, or any other provision of this chapter." 50 U.S.C. § 1881c(a)(2).

Shortly after the FAA was enacted, on August 18, 2008, the Attorney General sent DIRNSA a letter setting out the means by which FAA § 704 collection would be approved. Appendix 7A replaces that letter and provides that "[w]hen the Attorney General approves an application or authorizes an emergency acquisition" under FAA § 704 or related authorities, he is also "concurrently approving" the collection under Section 2.5.

Many of the provisions in Appendix 7A track the statutory requirements and do not require elaboration here. There are a few elements, however, that are worthy of note.

The first is a clear (and correct) requirement to "cease any acquisition" if "the target is reasonably believed to be in the United States." SA § 7A.3.a.(1). Unlike with collection under FAA § 702, there is no 72-hour emergency grace period for roamers. See 50 U.S.C. § 1805(f). To ensure that FBI-nominated targets are in fact abroad, the Annex requires the Bureau to provide written confirmation of that fact before commencing acquisition and to coordinate thereafter.

SA § 7A.9.a. This makes sense not because the FBI is unreliable, but because its focus is on domestic threats.

Section 7A.4 makes a noteworthy effort to describe the collection techniques that may be used under FAA § 704 and related provisions, but redactions make them hard to discern. They are as follows:

a. Surveillance using selection terms.

b. Computer surveillance (redacted).

c. Any other technique approved by the Attorney General.

None of these collection techniques may constitute "electronic surveillance" or a "physical search" as defined in traditional FISA. SA § 7A.4. In developing these collection methods, the USSS shall consider methods to limit collection of non-pertinent USPI, including "filtering non-pertinent information as soon as practicable after collection." SA 7A.4.d. Information is deemed "pertinent" if it "relate[s] to the target or is … relevant to the purpose of the collection." SA 7A.4A.d.

Finally, the Annex also contains an appropriate limit on reverse targeting, SA § 7A.5, which could in some cases amount to a fraud on the FISA Court. Cf. SA § 2.4.b. Sometimes, where the government has interests in multiple targets that share a single facility, close cases may be presented. Cf., e.g., *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280-281 (SDNY 2000), aff'd, 552 F.3d 157 (2d Cir. 2008). In such cases, the Annex provides that USSS personnel will consult with the Department of Justice. SA § 7A.5.

III. CONCLUSION

The SIGINT Annex is a very significant achievement. It updates the rules governing SIGINT to reflect constitutional, statutory, technological, and operational developments over the last three decades. It is amazing that the Prior Annex was last significantly modified in 1988, during the Reagan Administration, a decade after FISA and just two years after enactment of the Electronic Communications Privacy Act (ECPA). The time it has taken is a testament to the challenge of the task and the efforts of those who completed it.

The SIGINT Annex is flexible in many ways, but it also provides important limits on SIGINT activity that is not directly regulated by statute. In keeping with Executive Order 12333 and the Fourth Amendment, it primarily protects U.S. persons and persons in the United States. The relevant limits and protections for such persons include the following:

- Limits on "intentional targeting of U.S. persons or persons in the United States" (SA §§ 2.2.a, 2.5.b., 2.5.d.).

- Limits on intentional collection of domestic communications (SA § 2.4.a.).

- Requirements to use the "least intrusive means" for collection of USPI conducted within the United States or directed against a U.S. person abroad (SA § 2.2.a.(1) cross-reference), to collect no more USPI than is "reasonably necessary" (SA § 2.2.a.(1) cross-reference), and to consider methods to limit collection of non-pertinent USPI (SA § 2.3.a.(1)).

- Requirements to "make every reasonable effort" to "reduce, to the maximum extent possible," incidental collection of domestic communications and communications concerning U.S. persons (SA § 2.2.b.).

- Requirements to "consider" certain factors, such as "[m]ethods to limit the collection of [non-pertinent] USPI," in conducting SIGINT collection (SA § 2.3), and processing (SA § 3.2.a.(6)).

- Prohibitions on reverse targeting (SA §§ 2.4.b, 7A.5).

- Requirements to use selection terms for collection whenever practicable (SA § 2.2.a.(2)) and, where there is a risk that the selection terms will result in incidental collection of non-pertinent communications concerning U.S. persons, to take steps to defeat such collection, including collection of the communications themselves and of related data (SA 2.5.a.(1)).

- Requirements, when conducting SIGINT collection on foreign radio channels with a terminal in the U.S., to target non-U.S. persons abroad (and to use selection terms unless the channel is used exclusively by foreign powers) (SA § 2.5.a.(1)(a)).

- Requirements to conduct queries intended to retrieve communications concerning U.S. persons and persons in the United States only in certain circumstances (albeit a wide range of circumstances) (SA § 3.4).

- General requirements to destroy domestic communications, communications obtained by the inadvertent targeting of non-consenting U.S. persons, and communications of certain inadvertently targeted non-consenting non-U.S. persons in the United States (SA § 4.6).

- Requirements to minimize USPI in SIGINT disseminations (SA §§ 5.1 (cross-reference) 5.2, 5.3)

Although it is focused on U.S. persons and persons in the United States, the SIGINT Annex also provides important protections that extend to all persons, including non-U.S. persons located outside the United States, beyond those set forth in PPD-28. These protections include:

- Prohibitions on using foreign partners to accomplish something indirectly that the USSS cannot accomplish directly (SA § 1.3.b.) in keeping with Section 2.12 of Executive Order 12333. This is a significant limit because many foreign governments do not regulate SIGINT activity as rigorously or as transparently as does the United States.

- Limits on the purposes for which SIGINT collection (SA § 2.1) and querying (SA § 3.3) may be conducted.

- Requirements to "conduct targeted collection using selection terms whenever practicable" (SA § 2.2.a.(2)).

- Requirements to consider ways to limit collection to pertinent information (SA § 2.3.a. (2)) and ways to filter "non-pertinent information as soon as practicable after collection" (SA § 2.3.a.(3)).

- Requirements to comply with guidance issued by the Attorney General designed to protect attorney-client communications (SA § 1.3.e.).

- Limits on retention of unevaluated SIGINT (SA § 4.2). The purpose of this limit is mainly to protect U.S. persons and persons in the United States, but the limits operate to restrict retention in general because of the undifferentiated mixing of USPI and other information in unevaluated SIGINT.

- General requirements to destroy domestic communications of certain inadvertently targeted non-consenting non-U.S. persons in the United States (SA § 4.6.c.).

- Requirements for internal policies, compliance programs, training, auditing and internal controls, documentation, and reporting to external overseers (SA § 6) that help ensure actual compliance with stated laws and policies – another factor that may differentiate the United States from certain other governments.

Reasonable minds can certainly differ on whether the SIGINT Annex provides sufficient protections for U.S. persons, persons in the United States, and non-U.S. persons abroad. But its 35 pages of detail prescribe something very far removed from a wholly unrestricted approach.

In providing these protections and limits, as well as in authorizing SIGINT activity, the SIGINT Annex provides more clarity and prescription than its predecessor. In part, this reflects the changed environment in which it functions, and the trend towards greater regulation and transparency in SIGINT. But the SIGINT Annex still retains an operator's perspective and a focus on meeting mission needs. Indeed, one possible criticism of the new Annex is that it remains too anchored in legacy operations and relies too heavily on categories, conventions, and other traditional approaches that may be useful to those who do SIGINT for a living but may detract from clarity for those who do not. The balance between operational usefulness and theoretical

clarity is, however, an exceedingly difficult balance to strike, because the relevant audience for the SIGINT Annex includes both insiders and outsiders. I have tried, in this paper, to bridge the gap between them, providing an explanation of the SIGINT Annex that I hope will be helpful to anyone with a serious interest in this field.