

~~TOP SECRET//SI//ORCON//NOFORN~~

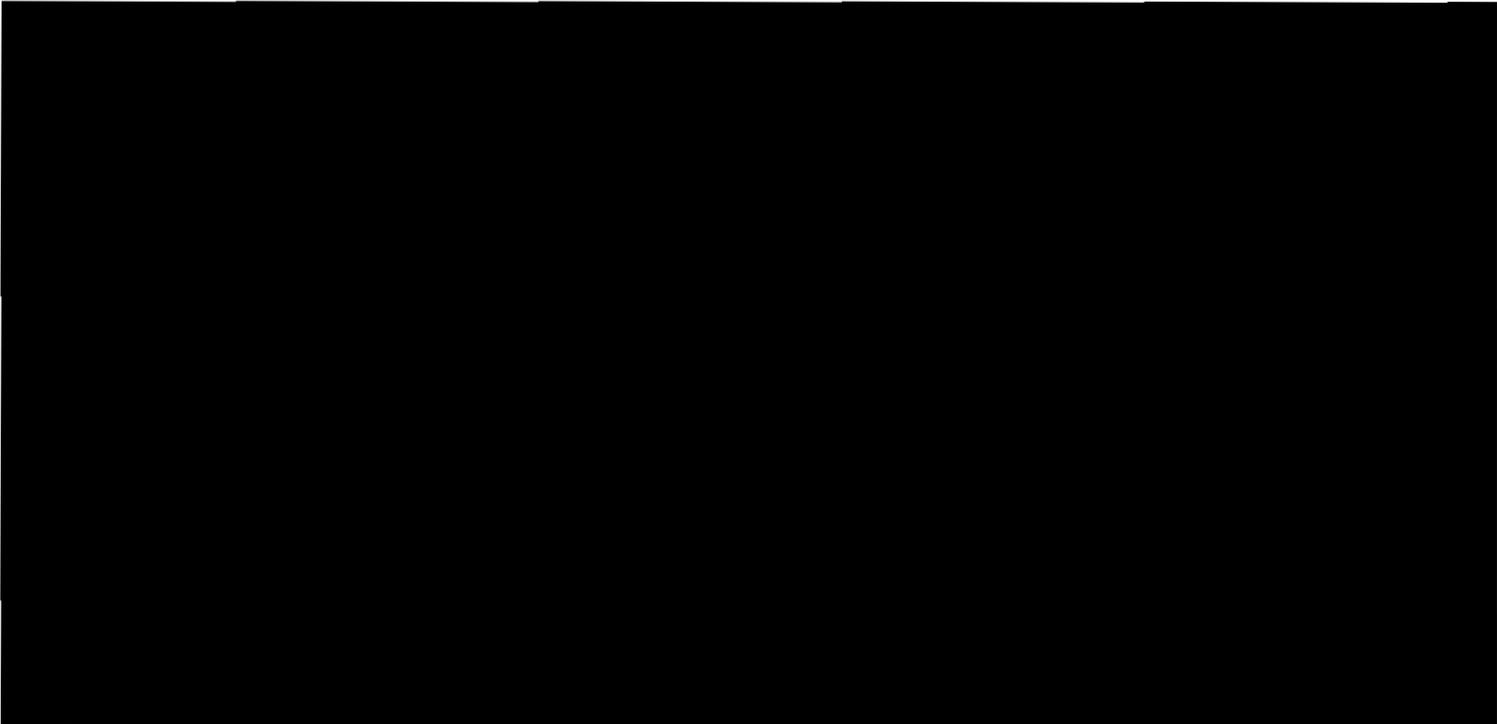
DEC 06 2019

UNITED STATES

LeeAnn Flynn Hall, Clerk of Court

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



**MEMORANDUM OPINION AND ORDER**

The Foreign Intelligence Surveillance Court today addresses the “Government’s Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications,” filed on September 17, 2019 (“September 17, 2019, Submission”). The September 17, 2019, Submission is subject to review by the Court under Section 702 of the Foreign Intelligence Surveillance Act (FISA) as amended, codified at 50 U.S.C. § 1881a. The government’s request for approval of the certifications and related procedures is *granted* for the

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

reasons stated in this Memorandum Opinion and Order, subject to certain reporting and other requirements set forth at the end of this document.

Part I of this Opinion summarizes the government's submissions and the procedural history of these matters. In Part II, the Court finds that the certifications before it contain the elements required by Section 702(h).

Part III addresses the targeting procedures, which include, among other changes, new provisions that require the National Security Agency and the Central Intelligence Agency to provide certain target-identifying information to the Federal Bureau of Investigation in connection with requests for the FBI [REDACTED]. The Court finds that those procedures, as written, satisfy the requirements of the statute.

The Court examines the proposed minimization procedures and querying procedures in Part IV. They include, among other changes, new provisions regarding user-activity monitoring activities by the FBI, CIA, and NSA. The Court finds that the procedures, as written, also satisfy the requirements of the statute.

In Part V, the Court evaluates the proposed procedures under the requirements of the Fourth Amendment and finds that, as written, they are consistent with those requirements. Part VI examines issues regarding implementation of, and compliance with, Section 702 procedures, including the FBI's progress in implementing recordkeeping and documentation requirements in the FBI's querying procedures, which came into effect upon the Court's approval on September 4, 2019. The Court concludes that the overall state of compliance and implementation permits a

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

finding that the procedures, as implemented, comport with statutory and Fourth Amendment requirements.

Finally, in Part VII, the Court summarizes its disposition and imposes certain reporting and other requirements on the government.

## I. PROCEDURAL HISTORY

### A. The 2019 Certifications and Amendments

The September 17, 2019, Submission includes [REDACTED] certifications executed by the Attorney General and the acting Director of National Intelligence pursuant to Section 702:

[REDACTED]

[REDACTED] Each of those certifications (collectively referred to as “the 2019 Certifications”) is accompanied by:

- (1) Supporting affidavits of the Director of the NSA, the Director of the FBI, the Director of the CIA, and the acting Director of the National Counterterrorism Center (NCTC);
- (2) Two sets of targeting procedures, which govern NSA and the FBI. The targeting procedures for NSA appear as Exhibit A to each certification, and those for the FBI appear as Exhibit C. The targeting procedures for each certification are identical;
- (3) Four sets of minimization procedures, which govern NSA, the FBI, the CIA, and NCTC respectively. The minimization procedures for NSA appear as Exhibit B to each certification, those for the FBI appear as Exhibit D, those for the CIA appear as Exhibit E, and those for NCTC appear as Exhibit G. (Exhibit F [REDACTED] identifies the individuals or entities targeted under those certifications [REDACTED]) The minimization procedures for each certification are identical; and
- (4) Four sets of querying procedures, which govern NSA, the FBI, the CIA, and NCTC respectively. The querying procedures for NSA appear as Exhibit H to each certification,

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

those for the FBI appear as Exhibit I, those for the CIA appear as Exhibit J, and those for NCTC appear as Exhibit K. The querying procedures for each certification are identical.

The September 17, 2019, Submission also includes an explanatory memorandum prepared by the Department of Justice (“September 17, 2019, Memorandum”).

The Court was initially required to review and rule on the certifications and procedures within 30 days of their submission – *i.e.*, by October 17, 2019. *See* § 702(j)(1)(B). On the government’s motion, and in order to allow for a full consideration of the issues presented, the Court extended this period by 60 days, until December 16, 2019, under Section 702(k)(2). *See* Order, Oct. 1, 2019. By order dated October 3, 2019, the Court further ordered the government to submit updates on certain compliance incidents that arose in connection with prior acquisitions under Section 702. Specifically, the Court required further information regarding: (i) NSA’s failure [REDACTED] as required by NSA’s targeting procedures [REDACTED]

[REDACTED] and steps that NSA was taking to remedy that failure; and (ii) NCTC and potentially other agencies’ failure to delete reports that were subject to recall by NSA for compliance or other reasons. *See* Order, Oct. 3, 2019. The government filed responsive submissions on November 4 and November 13, 2019.

**B. Subject Matter of the Certifications**

Each certification involves “the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information.”

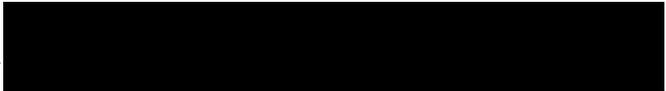
~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



The 2019 Certifications generally propose to continue acquisitions of foreign-intelligence information now being conducted under prior certifications that were initially submitted on March 27, 2018, and amended on September 18, 2018, and August 12, 2019 (“the 2018 Certifications”). See September 17, 2019, Memorandum, at 2-3. The 2018 Certifications are

 covering the same subjects as the 2019 Certifications.

The 2018 Certifications, in turn, generally renewed authorizations to acquire foreign-intelligence information under a series of certifications made by the AG and DNI pursuant to Section 702 that dates back to 2008. See Docket Nos. 

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Those docket, together with Docket Numbers  
are collectively referred to as “the Prior 702 Dockets.”

The government also seeks approval of amendments to the certifications in the Prior 702 Dockets, such that NSA, the CIA, the FBI, and NCTC henceforward would apply the same minimization and querying procedures to information obtained under prior certifications as they would to information to be obtained under the 2019 Certifications. See September 17, 2019, Memorandum

## II. REVIEW OF THE 2019 CERTIFICATIONS AND PRIOR CERTIFICATIONS, AS AMENDED

The Court must review a Section 702 certification “to determine whether [it] contains all the required elements.” § 702(j)(2)(A). Its examination of the 2019 Certifications confirms that:

(1) the certifications have been made under oath by the AG and the DNI, as required by § 702(h)(1)(A), see

(2) the certifications contain the attestations required by § 702(h)(2)(A),

(3) as required by § 702(h)(2)(B), each certification is accompanied by targeting procedures and minimization procedures adopted in accordance with § 702(d) and (e), respectively;

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(4) each certification is supported by affidavits of appropriate national-security officials, as described in § 702(h)(2)(C); and

(5) each certification includes an effective date in compliance with § 702(h)(2)(D) – specifically, the certifications become effective on October 17, 2019, or the date upon which the Court issues an order concerning the certifications under § 702(j)(3), whichever is later. See [REDACTED]

[REDACTED] (The statement described in § 702(h)(2)(E) is not required because there was no “exigent circumstances” determination under § 702(c)(2).)

The Court concludes that the 2019 Certifications contain all the required statutory elements. As to the first element, it finds that acting DNI Joseph Maguire was duly appointed to serve in that capacity by the President, and therefore was authorized to execute the certifications as the DNI under § 702(h)(1)(A). The President appointed Vice Admiral Maguire to serve as acting DNI after the resignations, effective August 15, 2019, of the DNI and Principal Deputy DNI. See September 17, 2019, Memorandum, at 2 n.1. At the time of such appointment, he had served as the Director of NCTC, with the confirmation of the Senate, since December 27, 2018. See *id.* He was eligible to be appointed acting DNI because he was serving “in an office [Director of NCTC] for which appointment is required to be made by the President, by and with the advice and consent of the Senate.” 5 U.S.C. § 3345(a)(2). (It appears that he was separately eligible for such appointment under § 3345(a)(3), but subsection (a)(2) suffices on its own.)

Similarly, the Court has reviewed the certifications in the Prior 702 Dockets, as amended by the 2019 Certifications, and finds that they also contain all the elements required by the statute. Those amendments have the same effective dates as the 2019 Certifications. See [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

The requisite procedural boxes having been checked, the Court will next review the proposed targeting, querying, and minimization procedures. The following discussion primarily focuses on proposed changes to the previously approved procedures, but the procedures as a whole must be consistent with statutory and constitutional requirements. Some technical, conforming edits and other changes are not specifically discussed because they raise no issues material to the Court's review.

### III. THE TARGETING PROCEDURES

Targeting procedures must be “reasonably designed” to “ensure that any acquisition authorized under [§ 702(a)] is limited to targeting persons reasonably believed to be located outside the United States” and to “prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” § 702(d)(1); see also § 702(b)(1) (acquisitions “may not intentionally target any person known at the time of acquisition to be located in the United States”); § 702(b)(4) (acquisitions “may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States”). Additionally, the government uses the targeting procedures to ensure that acquisitions do “not intentionally target a United States person reasonably believed to be located outside the United States.” § 702(b)(3). Pursuant to § 702(j)(2)(B), the Court assesses whether the targeting procedures satisfy those criteria. The Court must also determine whether the targeting procedures, along with the querying and minimization procedures, are consistent with the requirements of the Fourth Amendment. See § 702(j)(3)(A)-(B).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~**A. Background on Acquisition and Targeting Under Section 702**

The government targets a person under Section 702 by tasking for acquisition one or more selectors (*e.g.*, identifiers for email or other electronic-communication accounts) associated with that person. Section 702 encompasses different forms of acquisition. The government may acquire information “upstream,” as it transits the facilities of an Internet backbone carrier, as well as “downstream,” from systems operated by providers of services [REDACTED]. Traditional telephone communications may also be acquired upstream . . . .

[REDACTED] Mem. Op. and Order, Oct. 18, 2018,

at 11 (citation omitted) (“October 18, 2018, Opinion”).

NSA is the lead agency in making targeting decisions under Section 702. It may not task a selector without first determining that the target is reasonably believed to be a non-U.S. person outside the United States (a “foreignness determination”). In making such determinations, NSA reviews certain categories of information about the proposed target and evaluates “the totality of the circumstances based on the information available with respect to that person, including

[REDACTED] 2019 NSA

Targeting Procedures § I at 1. An NSA targeting decision must also be supported by a “particularized and fact-based” assessment that “the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information” relevant to the subject matter of an authorized Section 702 certification. *Id.* at 4.

NSA is also required to conduct post-targeting analysis “to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States is located in the United States.” 2019 NSA Targeting Procedures § II at 7. This post-targeting analysis involves routinely comparing each tasked selector against independently acquired

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 9

~~TOP SECRET//SI//ORCON//NOFORN~~

information for indications that a tasked selector may be used inside the United States, and examination of the content of communications obtained through surveillance of a tasked selector for indications that a targeted person is now in, or may enter, the United States. Id. at 6-7. If NSA concludes that a target is in the United States

Id. § II at 8, § IV at 10.

NSA tasks selectors for

The FBI is the agency responsible for

and in that role is

governed by its targeting procedures. Under those procedures, the FBI may

selectors that have already been approved for tasking by NSA

under its targeting procedures. See FBI Targeting Procedures § I.1. “Thus, the FBI Targeting

Procedures apply in addition to the NSA Targeting Procedures,”

See Docket No. Mem. Op., Sept. 4, 2008, at 20 (emphasis in original)

(“September 4, 2008, Opinion”).

NSA requests to the FBI and provides an explanation of its prior foreignness determination for each requested selector (or “Designated Account”). See FBI Targeting Procedures §§ I.1, I.2. The FBI, “in consultation with NSA, will review and evaluate the sufficiency of” that determination. Id. § I.3. The FBI also runs certain checks of information in its possession in the course of that review and evaluation. “Unless the FBI

that the user of the Designated Account is a United States person or is located inside

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

of the United States, the FBI will [REDACTED]

[REDACTED] Id. § I.5. “If the FBI [REDACTED] the Designated Account is not appropriate for tasking . . . , the FBI will inform NSA” and will not [REDACTED] that account unless and until it “determines that the Designated Account is in fact appropriate for tasking.” Id. § I.8.

**B.** [REDACTED]

The government proposes to modify a requirement in the current targeting procedures that NSA employ certain technical measures to ensure that at least one end of each acquired communication is outside the United States when it conducts Internet upstream collection. (In the following discussion, “upstream collection” refers to upstream acquisition of Internet communications under Section 702.)

The targeting procedures now in effect require NSA, when conducting upstream Internet collection, to [REDACTED]

[REDACTED] 2018 NSA Targeting Procedures § I at 2 (This

Opinion cites specific procedures now in effect under the 2018 Certifications in the form of “2018 [Agency] [Type of Procedures],” regardless of the date of any amendments— e.g., “2018 FBI Querying Procedures.” Specific procedures proposed for use under the 2019 Certifications are cited similarly, e.g., “2019 FBI Querying Procedures”). The government now seeks to lift that requirement in certain circumstances. For example, [REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]

The government asserts that, in such circumstances, the above-described requirement has resulted in the loss of foreign-intelligence information [REDACTED]

[REDACTED]

See September 17, 2019, Memorandum, at 9.

The government proposes to amend the NSA's targeting procedures so that [REDACTED]

[REDACTED]

See 2019 NSA Targeting Procedures § I at 2. The proposed change would "allow NSA to

[REDACTED] to or from a target [REDACTED]

September 17, 2019, Memorandum, at 10. Sections

702(b)(4) and 702(d)(1)(B) are concerned with whether "the sender and all intended recipients"

of a communication "are known . . . to be located in the United States," not with [REDACTED]

[REDACTED]

Because NSA, after applying its targeting procedures, must reasonably believe that a tasked facility is used exclusively by non-U.S. persons

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

outside the United States, this modification presents no impediment to the Court's approval of the 2019 NSA Targeting Procedures.

On some prior occasions when NSA had tasked [REDACTED] it violated its current targeting procedures [REDACTED]

[REDACTED] apparently in order to avoid loss of foreign-intelligence information. See Preliminary Notice of Compliance Incident Regarding [REDACTED]

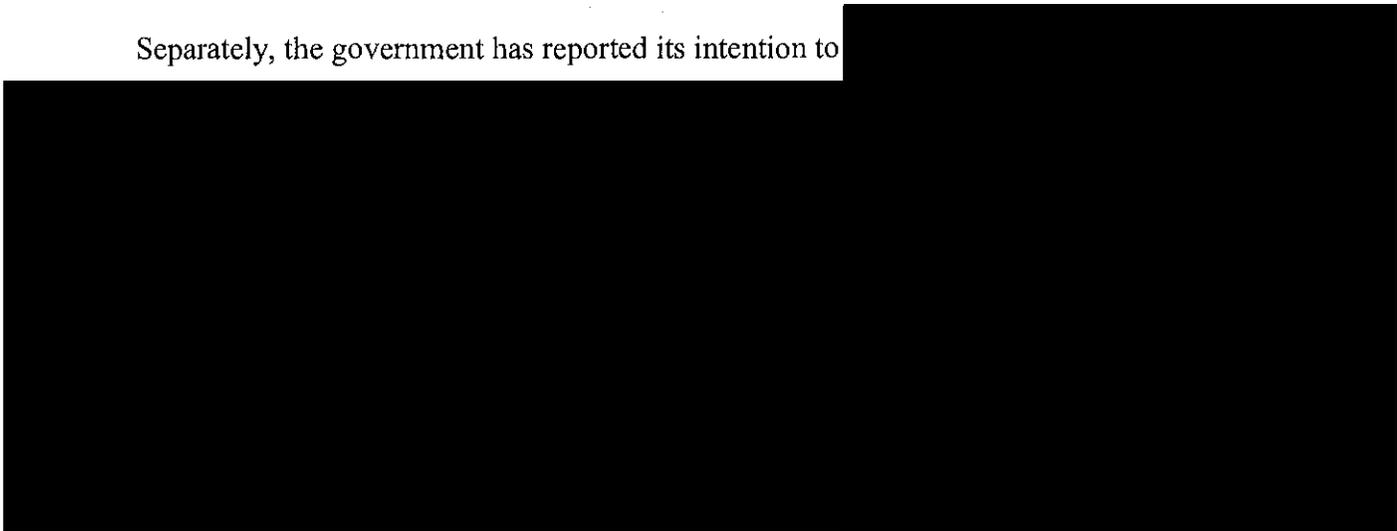
[REDACTED] Certain Upstream Acquisitions, Feb. 21, 2019. Of course, the proper course would have been to seek amendment of the procedures earlier, rather than unilaterally deciding to deviate from them. Indeed, the Court's October 3, 2019, Order required the government to provide additional information about the disposition of information that was improperly acquired as a result of that incident.

In a responsive submission filed on November 4, 2019, the government reported that NSA had failed to [REDACTED] prior to February 26, 2019, but had [REDACTED] as of that date. See Report in Response to the Court's Order Dated October 3, 2019, Nov. 4, 2019, at 2-3 ("November 4, 2019, Report"). The government reported that NSA identified [REDACTED] which might have resulted in the unauthorized acquisition of communications that did not originate or terminate outside the United States. Id. at 3. NSA has identified [REDACTED] resulting from such unauthorized acquisition and expects to have completely purged them by the end of January 2020. Id. at 5-6.

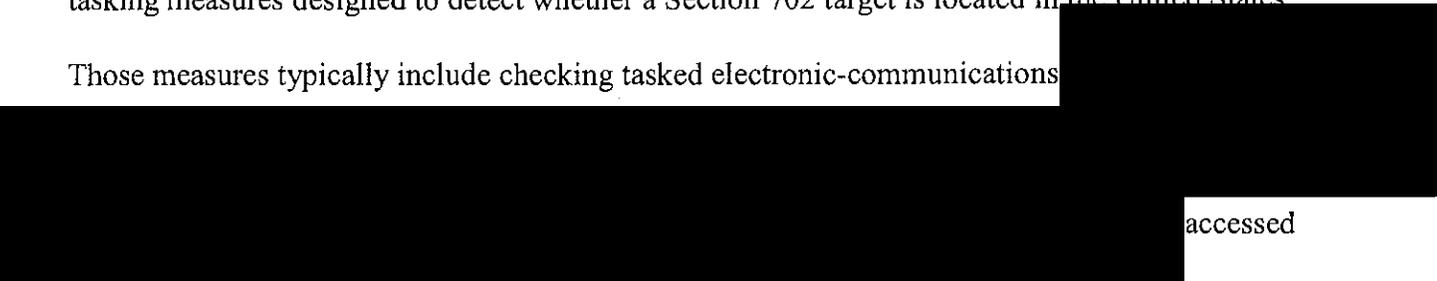
~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Separately, the government has reported its intention to



Downstream collection, conversely, is not subject to the above-described limitations, which apply only to upstream collection. But all Section 702 collection is subject to certain post-tasking measures designed to detect whether a Section 702 target is located in the United States. Those measures typically include checking tasked electronic-communications



accessed

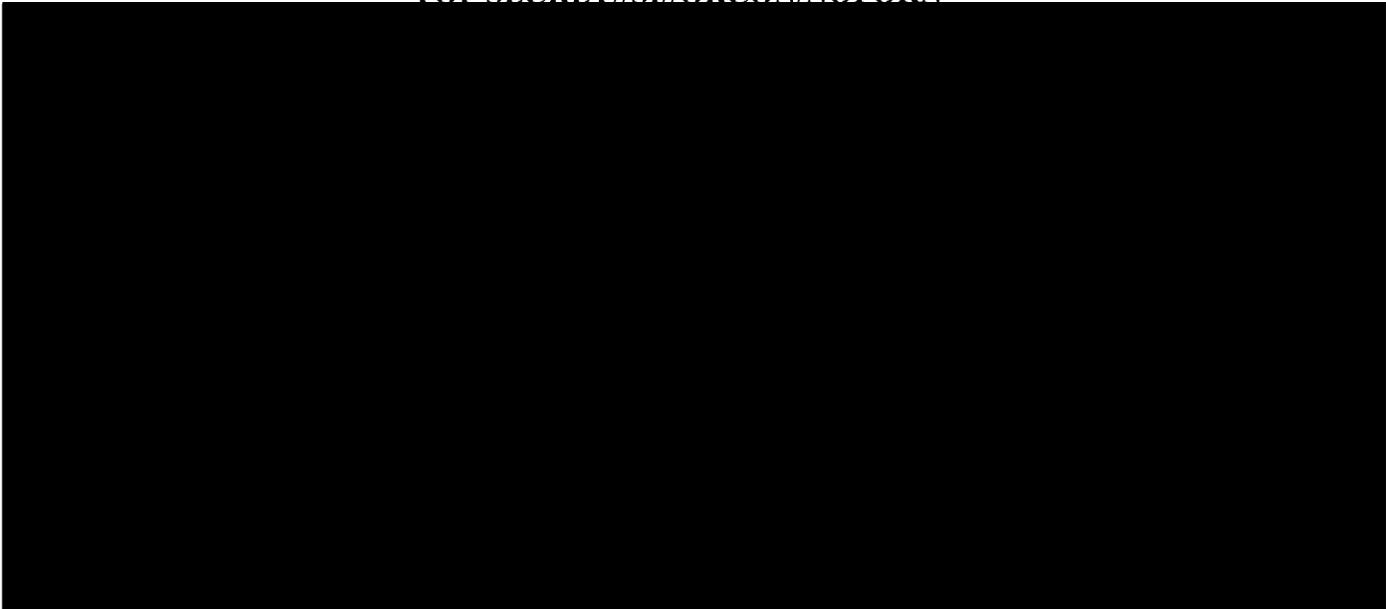
from inside the United States. See 2019 NSA Targeting Procedures § II.b at 7. The Notice filed on August 23, 2019, explains that post-tasking checks for selectors for certain would not result in useful information regarding the location of the targets who use those facilities. See August 23, 2019, Notice, at 2-3.



In anticipation of tasking such facilities, the proposed NSA targeting procedures have been revised to require post-tasking checks only “in those cases in which [NSA] is technically capable of” performing them. See 2019 NSA Targeting Procedures § II at 8.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



Id. at 8-9.

The Court expects that [redacted] post-tasking checks will be employed whenever feasible. On that understanding, and in view of the increased frequency with which acquired communications will be reviewed for indications that a target is in the United States when the [redacted] checks are not feasible, this revision does not impede the Court’s finding that the 2019 NSA Targeting Procedures are “reasonably designed to . . . ensure” that acquisitions are “limited to targeting persons reasonably believed to be located outside the United States.” § 702(d)(1)(A).

**C. Information Sharing for, and Evaluation of, [redacted] (FBI Procedures)**

The government has long had internal policies and practices for the passage of target-identifying information from NSA to FBI in connection with requests [redacted]

[redacted] for a tasked selector. [redacted] an instance where a target [redacted]

[redacted] was later determined to be a U.S. person, see Docket No [redacted]

Supplemental Order, July 25, 2017, at 3-4, the Court advised the government that it should [redacted]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

include greater detail about information sharing in the targeting procedures in order for the Court to better assess their adequacy and monitor compliance. The government has undertaken to do so in this submission.

**1. Steps Taken By NSA**

The proposed procedures require NSA to take additional steps before tasking a selector

[REDACTED]

under Section 702. See September 17, 2019, Memorandum, at 13.

Specifically, NSA will

[REDACTED]

Id. The FBI targeting procedures

have been revised to require that, “[p]rior to requesting that the FBI

[REDACTED]

NSA will

[REDACTED]

to determine

whether the user of the Designated Account

[REDACTED]

is a person reasonably believed to be located outside the United States and is not a United States person.” 2019 FBI Targeting Procedures § I.1.

As previously, the procedures require NSA to “provide the FBI with identifying information” of a Designated Account, together with “an explanation of NSA’s conclusion that the user” of the account is a non-U.S. person located outside the United States. Id. § I.2. NSA is now also expressly required to provide the FBI

[REDACTED]

“identifying information” for the user(s) of the Designated Account “obtained or identified by the NSA through application of its targeting procedures and determined to be reliable, including

[REDACTED]

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

additional identifying information of the user of the Designated Account, to the extent that NSA assesses it would be useful to FBI for purposes of application of [the FBI's targeting] procedures." Id.



Under these provisions, NSA has some discretion in determining what information is "reliable" or "useful," and therefore must be passed to the FBI. The Court expects NSA to make such determinations on an individualized, case-by-case basis, by assessing the totality of information available about a particular target or selector. In close cases, the Court expects NSA to err on the side of providing information to the FBI, rather than withholding it, so that the FBI is better able to make informed and accurate decisions under its targeting procedures.

The government reports that it will take time to implement these new information-sharing requirements, but has not provided an estimate of how much time. The Court views these requirements as important enhancements and expects them to be implemented expeditiously. The government has undertaken to report to the Court on such implementation every 45 days, and the Court intends to monitor closely the agencies' progress on implementing these new requirements.

In its first report, submitted on November 1, 2019, the government advised that NSA has



~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]

The agencies are continuing to discuss how to

pass relevant

information in a manner that is more conducive

Id. at 10-11.

Id. at

11-12. The agencies continue to discuss how other useful and reliable information might be identified and passed to the FBI.

The FBI expects to

“complete these system modifications within the same timeframe as NSA.” Id. at 13. The

agencies are also working on guidance and training for their personnel on these new procedures.

Id. at 13-14.

## 2. Steps Taken By the FBI

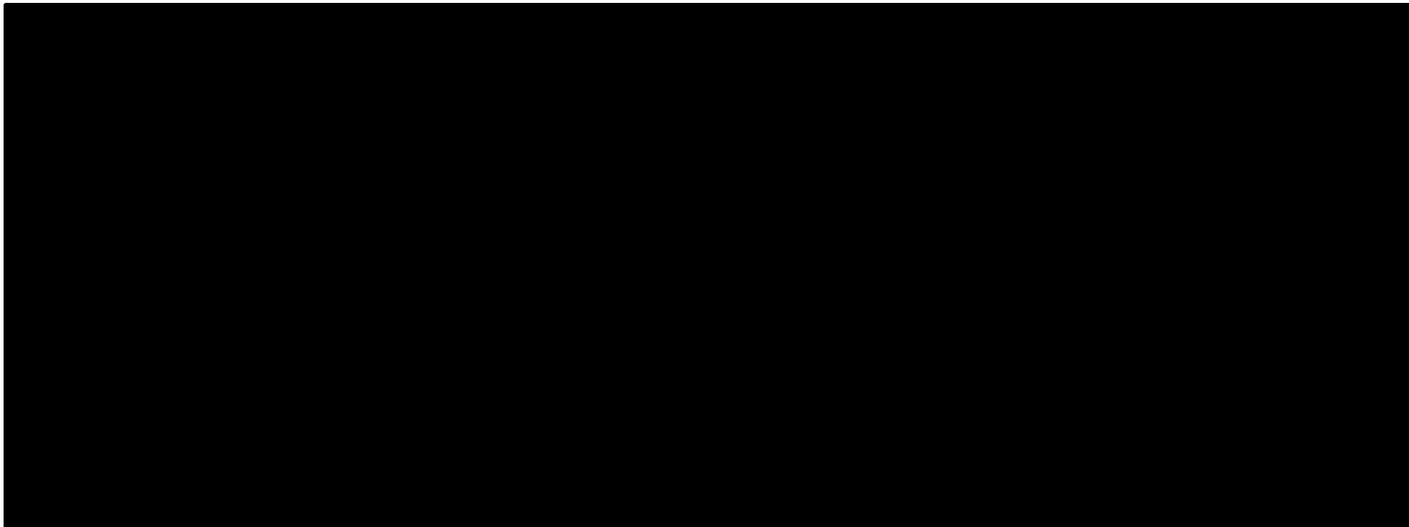
For its part, the FBI will consider this information in its review of the appropriateness of the tasking prior to the targeted selector. See FBI Targeting Procedures

§ 1.3.

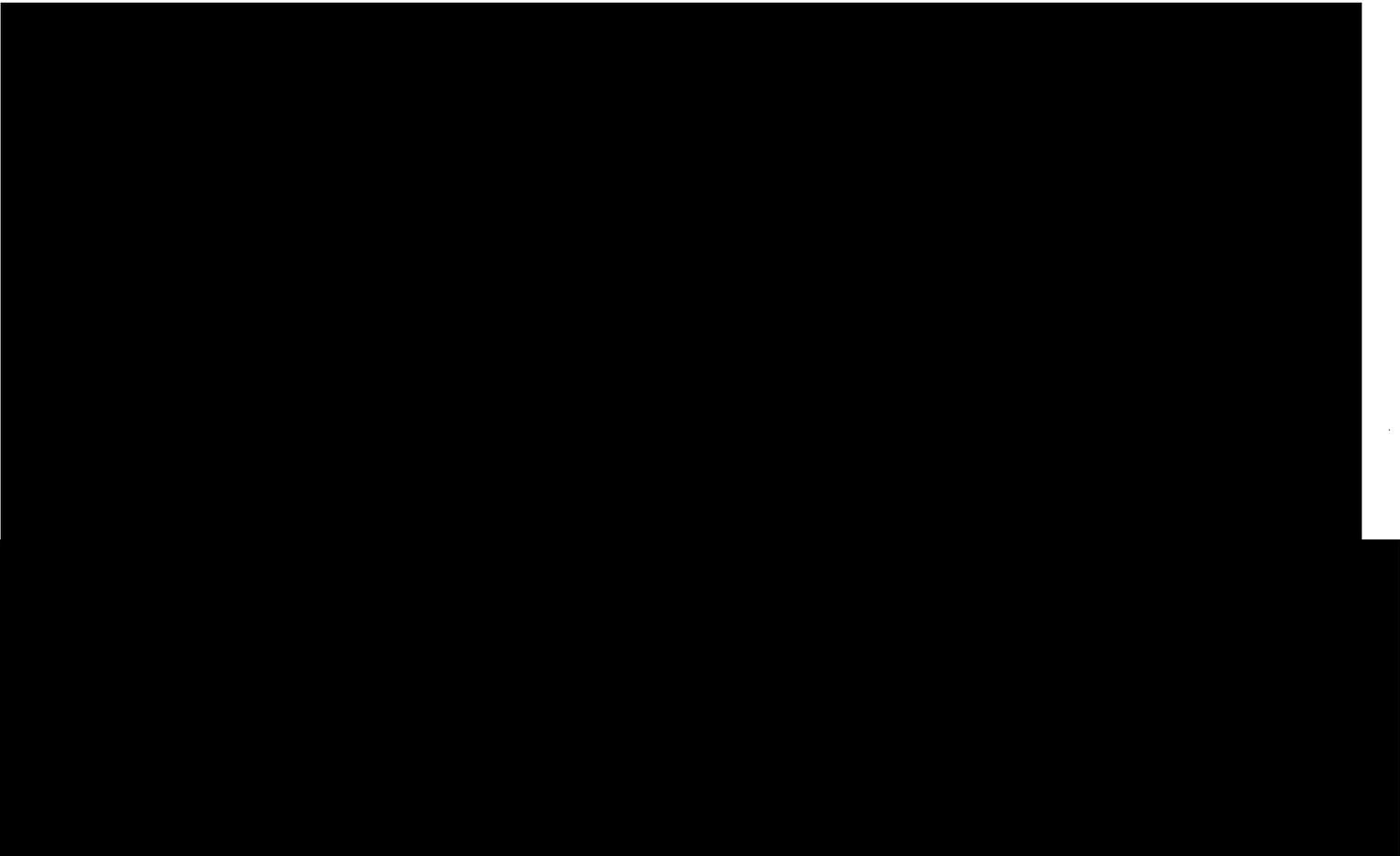
[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

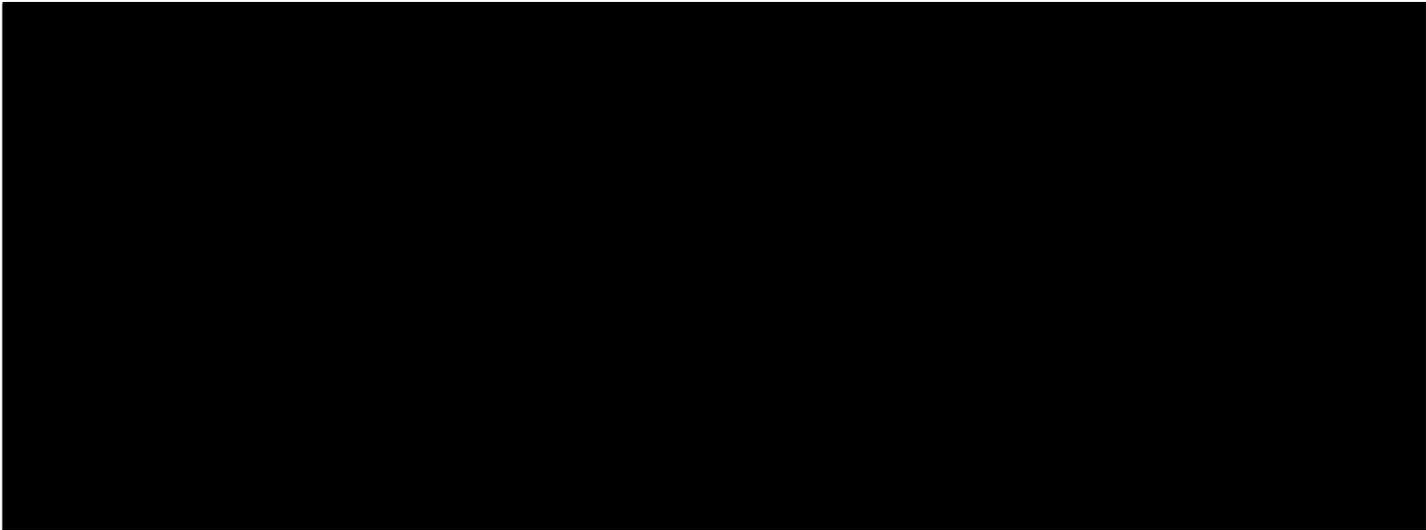


The proposed procedures provide greater detail about the searches to be conducted by the  
FBI. For example:



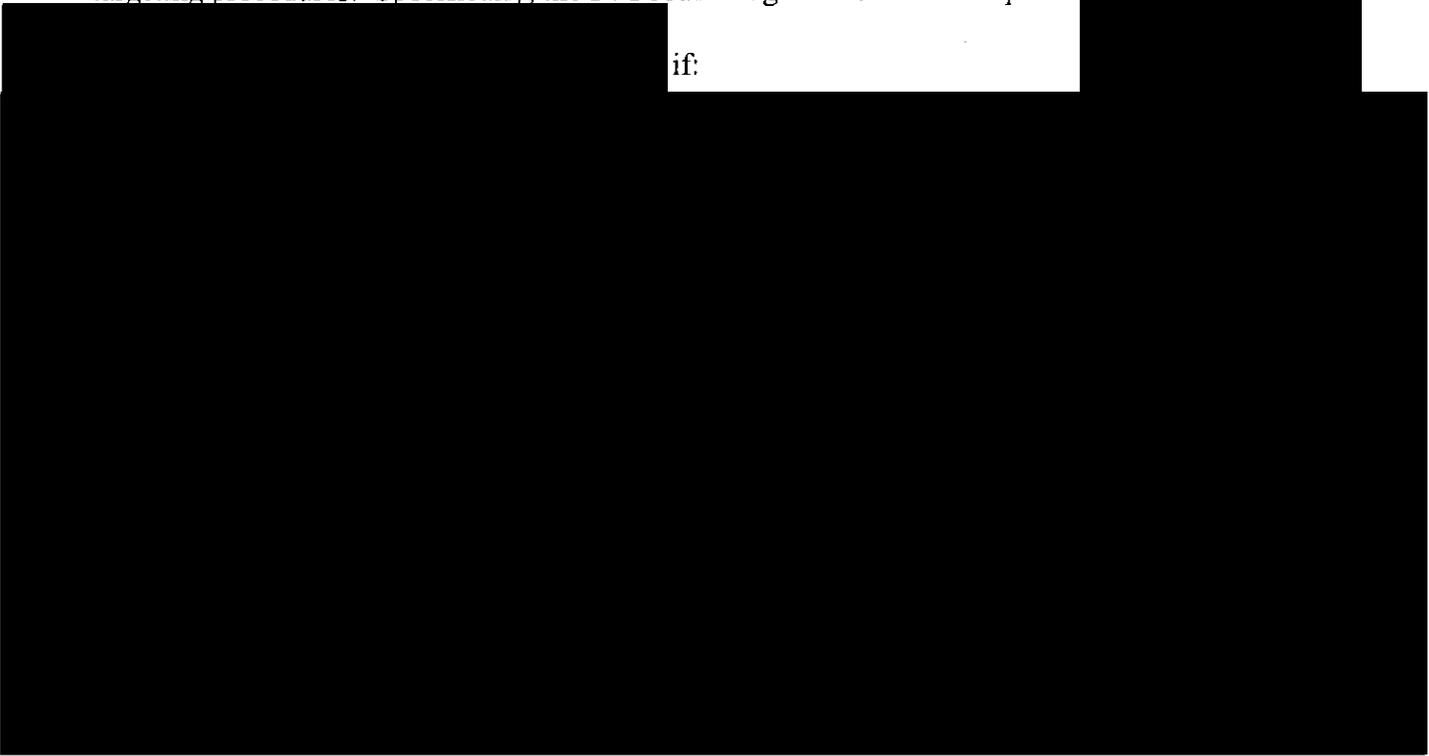
~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



The proposed procedures also include new provisions that, in specified circumstances, permit the FBI to forgo actions that would be otherwise required. The first provision concerns situations in which the Bureau would be permitted to rely on steps taken by NSA under its targeting procedures. Specifically, the FBI could forgo an otherwise required

if:



~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED]

One can conceive of circumstances in which omitting an FBI [REDACTED] under this provision could result in erroneous approval [REDACTED]

[REDACTED] On the other hand, it seems likely that, in the vast majority of situations in which the provision would be relied upon, the FBI would simply be avoiding duplicative effort that would not yield relevant new information.

Another new provision of the proposed procedures permits the FBI, when faced with “an immediate threat to human life or property,” to “immediately [REDACTED] of a Designated Account” requested by NSA without: a) reviewing and evaluating the sufficiency of NSA’s assessment that the target is a non-U.S. person located outside the U.S.; or b) conducting any queries in FBI systems. See 2019 FBI Targeting Procedures § I.4.h. The FBI would be required to take those steps “at the first available opportunity, but no later than the next business day.” Id. FBI must also notify the Department of Justice’s National Security Division (NSD) and the Office of the DNI (ODNI) , and NSD must notify the FISC. Id.

The government provided an example of an exigent circumstance involving a threat to [REDACTED]

[REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

The Court credits the government's proffered need to act without delay in such situations. But it must also be noted that Section V of the NSA targeting procedures similarly permits that agency, when faced with an immediate threat, to forgo steps and assessments it ordinarily is required to take before tasking [REDACTED]. If the same account were the occasion for departures by both agencies, it theoretically could be tasked [REDACTED]

[REDACTED] without any research regarding, or assessment of, whether the account's user is a non-U.S. person located outside the United States. NSA's emergency-departure provision requires the government to "continue to adhere to all of the statutory limitations set forth" in Section 702(b), so intentional targeting of U.S. persons or persons known to be in the United States would be prohibited, even in exigent circumstances. See 2019 NSA Targeting Procedures § V. And the requirement that the FBI take the otherwise required steps no later than the next business day and notification to NSD and ODNI, and ultimately the FISC, act as further checks against potential abuse of this provision. On balance, the Court finds it reasonable to approve this provision, on the expectation that it will be promptly informed of any circumstances in which it is invoked.

#### **D. Conclusion**

This Court has previously found the current versions of the FBI's and NSA's targeting procedures to comply with statutory requirements. See October 18, 2018, Opinion at 132. The above-described changes to those procedures, individually and taken together, do not undermine the bases for those prior findings. The modification to [REDACTED] NSA targeting procedures is a common-sense adjustment to limited situations [REDACTED]

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED] With the exception of the emergency-departure provision, the changes to the FBI's targeting procedures provide greater specificity regarding the protections against targeting U.S. persons or persons in the United States. Although the FBI need not conduct certain checks when they are likely to be redundant of steps recently taken by NSA, NSA now [REDACTED] before tasking a selector [REDACTED]. The net effect of those changes should be earlier detection of any indication that a proposed acquisition may concern a target who is a U.S. person or in the United States. The new information-sharing requirements should enhance the FBI's ability to research and evaluate whether a target is a U.S. person or in the United States [REDACTED].

The Court concludes, accordingly, that the 2019 NSA Targeting Procedures and the 2019 FBI Targeting Procedures, as written, are reasonably designed, as required by Section 702(d)(1), to: (1) ensure that any acquisition authorized under the 2019 Certifications is limited to targeting persons reasonably believed to be located outside the United States, and (2) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, moreover, it concludes that the NSA and FBI Targeting Procedures, as written, are reasonably designed to prevent United States persons from being targeted for acquisition – a finding that is relevant to the Court's analysis of whether those procedures are consistent with the requirements of the Fourth Amendment. See pages 57-61 infra.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

#### IV. THE MINIMIZATION PROCEDURES AND QUERYING PROCEDURES

Pursuant to § 702(j)(2)(C), the Court must assess whether the minimization procedures comply with specified statutory requirements. Section 702(e)(1) requires that the procedures “meet the definition of minimization procedures under [50 U.S.C. § 1801(h) or 1821(4)].” That definition requires

(1) specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], to minimize the acquisition and retention, and 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;

(2) procedures that require that nonpublicly available information, which is not 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; [and]

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]

§ 1801(h). The definition of “minimization procedures” at § 1821(4) is substantively identical to the definition at § 1801(h) (although § 1821(4)(A) refers to “the purposes . . . of the particular physical search”). For simplicity, subsequent citations refer only to § 1801(h).

In applying these statutory requirements, the Court is mindful that Section 702 acquisitions target persons reasonably believed to be non-U.S. persons outside the United States. Although such targets may communicate with or about U.S. persons, Section 702 acquisitions, as a general matter, are less likely to acquire information about U.S. persons that is unrelated to the

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

foreign-intelligence purpose of the acquisition than, for example, electronic surveillance or physical search of a home or workplace within the United States that a target shares with U.S. persons. Different minimization protections may be appropriate for other forms of collection that are directed at persons within the United States.

The AG, in consultation with the DNI, also must “adopt querying procedures consistent with the requirements of the fourth amendment . . . for information collected” pursuant to a Section 702 certification, see § 702(f)(1)(A), and must “ensure” those procedures “include a technical procedure whereby a record is kept of each United States person query term used for a query.” § 702(f)(1)(B). The FISC must determine whether querying procedures satisfy the requirements of § 702(f)(1). See § 702(j)(3)(A)-(B).

Each agency’s procedures make clear that the querying and minimization procedures are to be read and applied together. See, e.g., 2019 NSA Querying Procedures § I (“These querying procedures should be read and applied in conjunction with [the separate] minimization procedures, and nothing in these procedures permits any actions that would otherwise be prohibited by those minimization procedures.”); 2019 FBI Querying Procedures § I at 1 (same); 2019 NSA Minimization Procedures § I at 1 (“These minimization procedures apply in addition to separate querying procedures. . . . [They] should be read and applied in conjunction with those querying procedures, and nothing in these procedures permits any actions that would otherwise be prohibited by those querying procedures.”); 2019 FBI Minimization Procedures § I.A at 1 (same). The Court will accordingly also assess whether each agency’s querying procedures, in conjunction with the minimization procedures, satisfy the standard of § 1801(h).

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

**A. Background on Section 702 Minimization and Querying**

Each agency with access to “raw,” or unminimized, information obtained under Section 702 (NSA, FBI, CIA, and NCTC) is governed by its own set of minimization procedures in handling that information. This opinion uses the terms “raw” and “unminimized” interchangeably. The NCTC Minimization Procedures define “raw” information as:

section 702-acquired information that (i) is in the same or substantially the same format as when NSA or FBI acquired it, or (ii) has been processed only as necessary to render it into a form in which it can be evaluated to determine whether it reasonably appears to be foreign intelligence information or to be necessary to understand foreign intelligence information or assess its importance.

2019 NCTC Minimization Procedures § A.3.d at 2.

There are significant differences among the various sets of minimization procedures based on factors such as the agencies’ differing missions, legal and policy constraints, and technical infrastructure, but they share several important features in common. Regarding acquisition, NSA is required to conduct acquisitions “in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.” 2019 NSA Minimization Procedures § 4(a) at 5. The FBI must follow its targeting procedures in conducting acquisitions. See 2019 FBI Minimization Procedures § II.A.1 at 6. (As discussed above, NSA and the FBI are the only agencies that conduct Section 702 acquisitions, and the FBI applies its targeting procedures to, and acquires data for, only selectors that NSA has approved for tasking under its targeting procedures. See pages 9-11 supra.)

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Post-acquisition, in broad outline, each agency's procedures:

- set criteria for the indefinite retention of information of or concerning United States persons and generally applicable timetables for destroying information that does not meet those criteria, see 2019 NSA Minimization Procedures § 4; 2019 FBI Minimization Procedures §§ III.C.b, III.D.4, III.E.4; 2019 CIA Minimization Procedures §§ 2, 3; 2019 NCTC Minimization Procedures § B.2, B.3;
- provide special rules for protecting attorney-client communications, see 2019 NSA Minimization Procedures § 5; 2019 FBI Minimization Procedures §§ III.D.5, III.E.6; 2019 CIA Minimization Procedures § 7.a; 2019 NCTC Minimization Procedures § C.5;
- set standards and procedures for disseminating information, see 2019 NSA Minimization Procedures §§ 6, 7(b); 2019 FBI Minimization Procedures § IV; 2019 CIA Minimization Procedures §§ 5, 7.c; 2019 NCTC Minimization Procedures § D; and
- prescribe procedures for obtaining technical or linguistic assistance from other agencies and/or from foreign governments, see 2019 NSA Minimization Procedures § 9(b); 2019 FBI Minimization Procedures § IV.D; 2019 CIA Minimization Procedures § 7.b; 2019 NCTC Minimization Procedures § D.5.

The procedures also speak to situations in which the government reasonably believed at the time of acquisition that the target was a non-U.S. person outside the United States, when the target was in fact a U.S. person or was inside the United States. The Court has concluded that the government is authorized to acquire such communications under Section 702. See September 4, 2008, Opinion at 25-27. Nonetheless, the procedures of each agency require destruction of information obtained under those circumstances, unless the head of the agency authorizes its retention after making certain findings for the specific information to be retained. See 2019 NSA Minimization Procedures § 4(d); 2019 FBI Minimization Procedures § III.A.3; 2019 CIA Minimization Procedures § 8; 2019 NCTC Minimization Procedures § B.4.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 27

~~TOP SECRET//SI//ORCON//NOFORN~~

In addition, each agency's querying procedures contain recordkeeping requirements for the use of U.S.-person query terms in response to § 702(f)(1)(B). See 2019 NSA Querying Procedures § IV.B; 2019 FBI Querying Procedures § IV.B; 2019 CIA Querying Procedures § IV.B; 2019 NCTC Querying Procedures § IV.B. They permit investigative and analytical personnel at the CIA, NSA, and NCTC to conduct queries of unminimized Section 702 information if the queries are reasonably likely to return foreign-intelligence information. See 2019 NSA Querying Procedures § IV.A; 2019 CIA Querying Procedures § IV.A; 2019 NCTC Querying Procedures § IV.A. Their FBI counterparts may conduct such queries if they are reasonably likely to return foreign-intelligence information or evidence of a crime. 2019 FBI Querying Procedures § IV.A. The FBI's querying procedures are further discussed at pages 61-71 infra.

Changes to the agencies' minimization procedures and querying procedures are discussed in the following sections.

**B. Provisions Relating to User-Activity Monitoring Activities**

User-activity monitoring (UAM) activities monitor use of an agency's own networks and systems to protect against misuse by employees and other persons with access to those systems. As explained below, some UAM activities are likely to capture and store a limited amount of unminimized 702 information. The proposed minimization procedures and querying procedures for the FBI, NSA, and CIA contain new provisions addressing UAM activities. Some background information regarding UAM activities will be helpful in examining those provisions.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

## 1. Background on UAM Activities

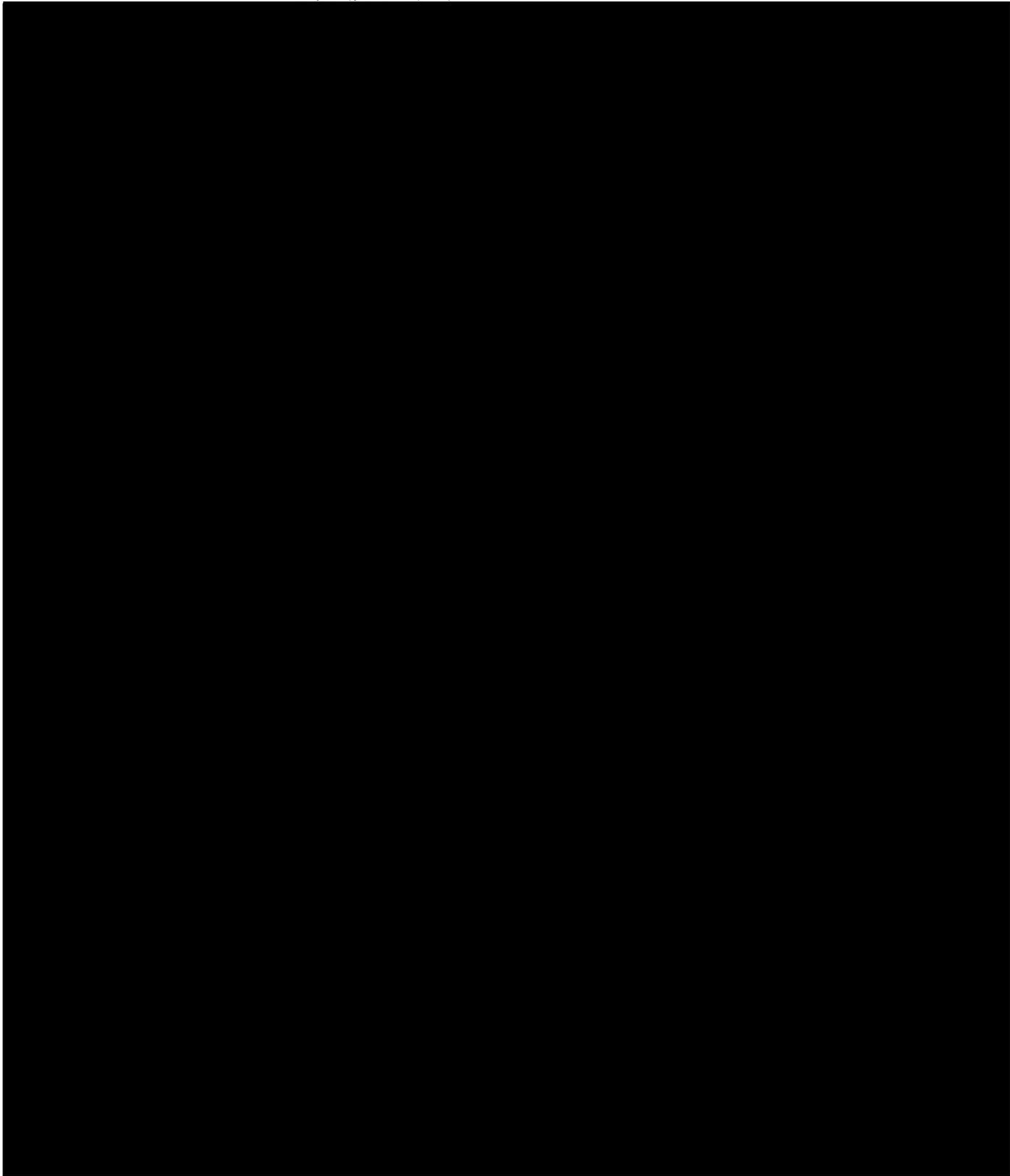
In connection with its submission of the 2018 Certifications, the government informed the Court that it had identified certain UAM activities, [REDACTED] and the subsequent placement of that information into systems maintained by insider-threat personnel.” October 18, 2018, Opinion at 130. [REDACTED]

During the Court’s consideration of the 2018 Certifications, the government was investigating the extent to which the agencies’ UAM activities copy and store raw Section 702-acquired information and thereby implicate minimization and querying rules. The Court accepted the government’s suggestion that it submit reports addressing how the UAM activities of each agency bear on Section 702 information. *Id.* at 131-32. The government submitted those reports on March 29, 2019.

They explain that the CIA, NSA, and FBI “routinely conduct consensual monitoring of their classified and unclassified computer systems to ensure that the systems remain secure and that sensitive information that is transmitted, stored, or processed on the systems is not used for unauthorized purposes.” September 17, 2019, Memorandum, at 37. [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

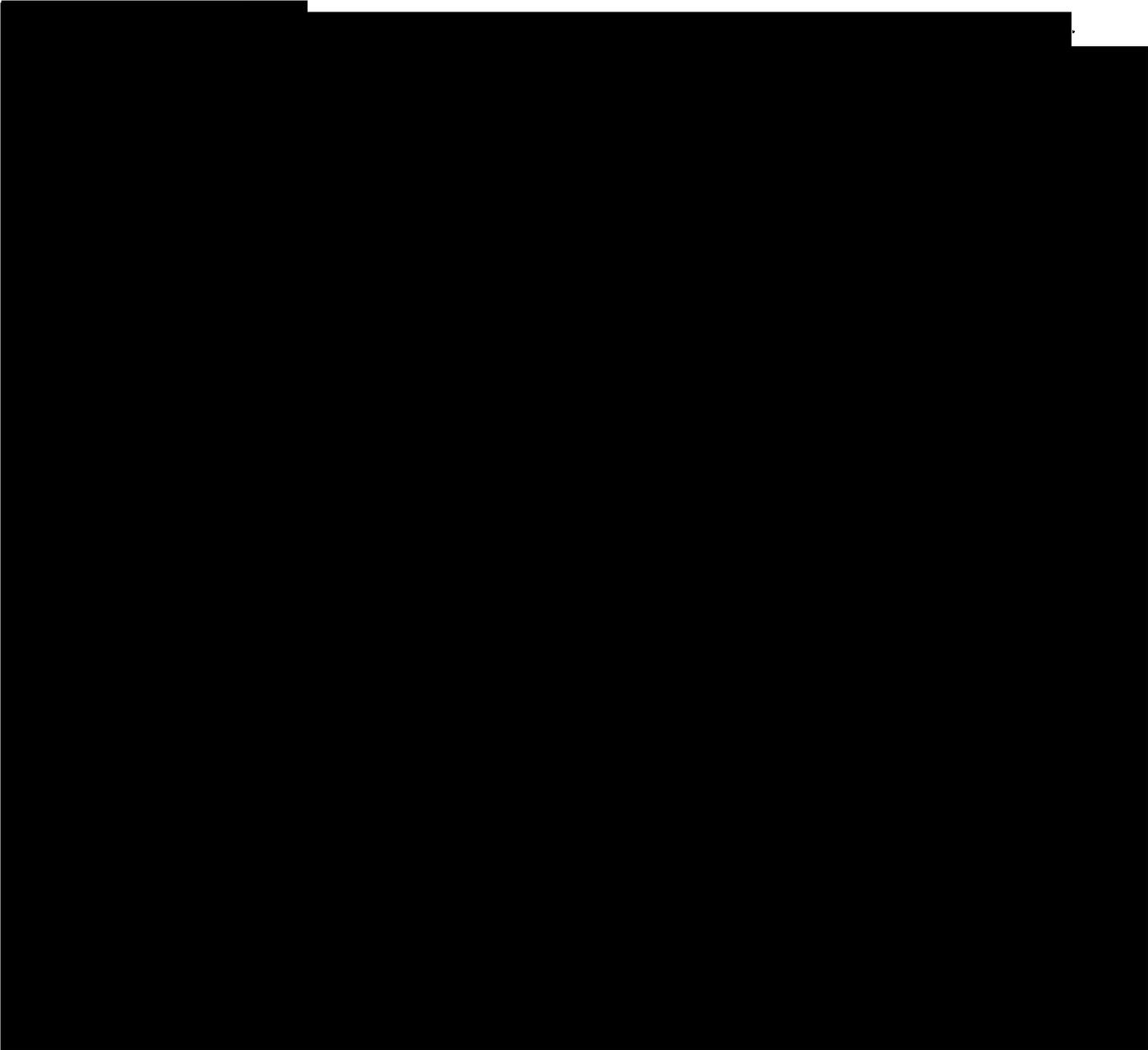


~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~



The CIA, NSA, and FBI all conduct certain forms of monitoring routinely, as well as



~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

The government describes its understanding that the agencies' UAM activities are authorized by various statutes, see NSA UAM Submission at 7-11 (discussing, among other provisions, 50 U.S.C. § 3232(a) and the National Defense Authorization Act for Fiscal Year 2012 § 922, Pub. L. 112-81), as well as by Executive Order No. 13587 and guidance issued thereunder. See id. at 11-15. The government does not argue that those authorizations render FISA's minimization requirements inapplicable. Id. at 16-18. It does, however, contend that this "legal framework . . . reflects the government's strong interest in deterring and detecting insider threats, including the safeguarding of classified information from exploitation or other unauthorized disclosure." September 17, 2019, Memorandum, at 40. The Court accepts that the FBI, CIA, and NSA legitimately need to safeguard classified information against insider threats, including unminimized Section 702 information.

A final observation is in order before turning to the proposed procedures. UAM activities acquire information about the users of the systems monitored and therefore may be thought to

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

implicate their privacy interests. But balancing *those* privacy interests against the need to guard against insider threats is not a task for this Court. The statute requires minimization procedures “for acquisitions authorized under” Section 702(a) and querying procedures “for information collected pursuant to an authorization under” Section 702(a). See § 702(e)(1), (f)(1)(A). Information about the conduct of users of agency systems recorded by UAM activities – e.g., that John Doe downloaded a particular file – is neither an acquisition authorized under Section 702(a) nor information collected pursuant to such an authorization, regardless of whether the downloaded file happened to contain Section 702-acquired information. The Court’s responsibility is to determine whether the procedures properly protect private U.S.-person information that was acquired pursuant to a Section 702 authorization, which is typically found in Section 702-acquired communications to which a U.S. person is a party or that discuss a U.S. person.

## 2. Minimization Provisions for UAM Activities

The proposed minimization procedures have protections against the improper use of Section 702 information in UAM systems, including limiting access and use of information to personnel involved in the agency’s insider threat mission. Specifically for each agency:

FBI The FBI’s proposed procedures permit retention of Section 702-acquired information in UAM systems only in furtherance of authorized UAM purposes. See 2019 FBI Minimization Procedures § III.F.7. Such information may only be accessed by authorized personnel [REDACTED] with UAM duties who have been trained on the procedures. Id. Such personnel may search UAM systems to “assist in insider threat inquiries or

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

investigations;

If FBI personnel identify

unminimized Section 702 information in a UAM system, they must remove it from the system unless (1) it meets generally applicable retention criteria and is not otherwise subject to purge; or (2) it is necessary to retain it for a UAM purpose, in which case the retention, and the reason therefor, must be included in the next quarterly report to the Court on Section 702 compliance matters, and the FBI must delete the information when it is no longer needed for a UAM purpose.

Id.

CIA The proposed provisions for the CIA's retention and use of Section 702-acquired information in UAM systems are materially the same as those described above for the FBI. See 2019 CIA Minimization Procedures § 7.e.

NSA. The proposed NSA minimization procedures would permit indefinite retention of unminimized Section 702-acquired information in NSA's UAM systems. See 2019 NSA Minimization Procedures § 10. NSA may use such information "solely to deter, detect, and otherwise protect against unauthorized access and use of NSA's systems and networks." Id. Access to such UAM systems is limited to personnel with UAM duties.

who have been trained on the procedures. Id.

~~TOP SECRET//SI//ORCON/NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Unlike the FBI and CIA, NSA would not be required in any circumstances to remove unminimized Section 702 information from a UAM system. NSA's UAM systems are not capable of "aging off data at set intervals or deleting individual records." NSA UAM Submission at 17; accord September 17, 2019, Memorandum, at 46. The Court understands that lack of capability to have resulted from a policy determination that "it is critical for [NSA's] UAM personnel to retain all of the information stored in its UAM repositories indefinitely." NSA UAM Submission at 17. In addition, even the FBI and CIA would not be required to systematically review their UAM systems to find any unminimized Section 702-acquired information and, if they discover such information on a UAM system, they may retain it there for as long as doing so serves a UAM purpose, subject to the above-described reporting requirement. The government contends that these relatively lax retention standards are justified because "it may take years to detect an insider threat, and once detected, UAM personnel will likely need to review older information captured through UAM processes with new context." September 17, 2019, Memorandum, at 41.

The Court finds that rationale persuasive, in the context of the limited amount of unminimized Section 702 information likely to be contained in UAM systems, the limited number of personnel with access to those systems, and the limited purposes for which such systems are used. The government's reporting on how UAM systems are currently configured and operated indicates that such access restrictions are largely in place. See, e.g., [REDACTED] Declaration at 21 (access to NSA's UAM data is controlled and accessible only to a limited number of authorized personnel); CIA UAM Submission at 12-13 (CIA's UAM repositories are

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

access-restricted [REDACTED]

and available for audit).

In response to an inquiry by the Court, the FBI recently indicated that [REDACTED]

[REDACTED] Authorized users will have access only to the information required to perform their official duties. *Id.* It is anticipated that the total number of users who may have access to the system will be [REDACTED] all of whom will have completed training on the FBI's FISA minimization procedures. *Id.* The Court accordingly concludes that the provisions of the proposed FBI, CIA, and NSA minimization procedures regarding the retention and use of information in UAM systems satisfy the requirements of 50 U.S.C. § 1801(h).

### 3. Exclusion of Searches of UAM Systems From Querying Procedures

The government proposes to exclude searches of agency systems from the definition of a “query” for purposes of the querying procedures for the FBI, CIA, and NSA, “so long as the only unminimized section 702-acquired information that the searches run against are in records captured through user activity monitoring.” NSA Querying Procedures § III.A; FBI Querying Procedures § III.A; CIA Querying Procedures § III.A.

For purposes of Section 702 querying procedures, FISA defines “query” as “the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized” under Section 702(a). *See* § 702(f)(3)(B). The government submits that searching a UAM system does not involve a “query” under that definition because such a search

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

must have a UAM purpose. (Recall that the proposed minimization procedures require any search of a UAM system that contains unminimized Section 702 information to have a UAM purpose.) And, in the government's view, any search for a UAM purpose would not involve the *use* of one or more terms *to retrieve* unminimized communications of or concerning U.S. persons obtained under Section 702 and therefore would not be a query as defined by the statute. See September 17, 2019, Memorandum, at 49-53. The Court concludes that it is permissible to exclude searches of UAM systems for UAM purposes from the querying procedures, but its analysis deviates somewhat from the government's arguments.

The government relies on a statement in the legislative history of Section 702(f) that "query refers only to retrievals of 'of or concerning United States persons,' and, therefore, the new querying procedures requirement does not apply to queries that are not specifically intended to return communications 'of or concerning United States persons.'" H.R. Rep. No. 115-475 part I, at 18 (2017) (cited by September 17, 2019, Memorandum, at 49 n.29). At the same time, however, the government concedes that the lack of a subjective intent to retrieve unminimized Section 702-acquired information does not necessarily mean that no query has occurred: it regards the use of terms to search the *main repositories* of unminimized Section 702 information as a "query," even if the person conducting it did not intend to search Section 702 information, but rather did so by mistake. Id. at 50 n.30. In the government's view, searching "analytical repositories . . . designed to store unminimized FISA-acquired information" justifies imputing the personnel who conducted the search "with the degree of intent necessary to trigger the statutory definition of query." Id.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

In the Court's assessment, searches of UAM systems conducted for UAM purposes and otherwise in compliance with applicable minimization requirements (hereinafter "UAM searches") are unlikely to retrieve unminimized U.S.-person communications. That is due in part to the fact that UAM systems contain a limited amount of unminimized Section 702 information, particularly in comparison to the main repositories of such information. The nature of the UAM purposes for which such searches are conducted also supports that assessment. Those purposes focus on the conduct of users of agency systems, not on U.S.-person communications contained within such raw Section 702 data as was incidentally copied in the course of UAM. Based on the same considerations, moreover, the Court assesses that it is not reasonable to regard UAM searches as intended to retrieve unminimized U.S.-person communications that were acquired under Section 702.

The Court concludes that searches of government systems that are neither likely to retrieve such unminimized communications nor intended to do so fall outside the statutory definition of "query." First, it would be an odd reading of the statutory text to conclude that a search involved "the use of one or more terms to retrieve" such communications, even though the search was not likely to retrieve them and the person running it did not intend to retrieve them. It would be anomalous, moreover, for unlikely and unintended search results to compel an after-the-fact conclusion that a particular search was a "query," particularly in view of requirements that agency personnel can satisfy only before they run a query. See, e.g., 2019 CIA Querying Procedures § IV.A ("Each query of CIA systems . . . must be reasonably likely to retrieve foreign intelligence information . . . unless otherwise specifically excepted in these procedures.").

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Finally, it is congruent with the purpose of Section 702(f) to conclude that the statutory definition of “query” does not encompass searches that are neither likely nor intended to return unminimized U.S.-person communications obtained under Section 702. Querying procedures must be “consistent with the requirements of the fourth amendment.” Section 702(f)(1)(A). The legislative history underscores the connection between the requirement to adopt querying procedures and Fourth Amendment concerns:

The [House Permanent Select Committee on Intelligence] is dedicated to providing assurances to the American public that the procedures and processes currently in place satisfy the Fourth Amendment, and do not impede on United States person privacy. Therefore, the Committee believes that the Intelligence Community should have separate procedures documenting their current policies and practices related to the querying of lawfully acquired FISA Section 702 data.

H.R. Rep. No. 115-475 part I, at 17-18. (The Court adverts to this legislative history for aid in resolving any ambiguity regarding the statutory definition of “query.”) The more specific statutory requirements for queries of Section 702 information are naturally understood as means chosen by Congress to further the ends of ensuring and demonstrating compliance with the Fourth Amendment and due protection of U.S. persons’ privacy. For example, Section 702(f)(2) (discussed further at pages 69-73 *infra*), requires the FBI to obtain a probable cause-based order from the FISC before examining the results of certain queries conducted using U.S.-person query terms in support of a predicated criminal investigation. The Foreign Intelligence Surveillance Court of Review has stated that “Section 702(f)(2), it appears to us, is intended to address . . . compliance with the Fourth Amendment” and “to avert any constitutional challenge to the FBI’s conduct,” particularly “in everyday criminal investigations unrelated to national security and foreign intelligence needs.” Docket No. 18-03, In re DNI/AG 702(h) Certifications 

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED] at 29 (FISCR July 12, 2019) (per curiam)

(“In re DNI/AG Certifications”).

Queries of the main repositories of unminimized Section 702 information substantially implicate Fourth Amendment interests, particularly when U.S.-person query terms are used. The targets of acquisition under Section 702 are reasonably believed to be non-U.S. persons outside of the United States, and those acquisitions have a significant purpose of acquiring foreign-intelligence information. See pages 8-11 supra; § 702(h)(2)(A)(v). But the use of U.S.-person identifiers to query the main repositories of unminimized Section 702 information indicates an interest in retrieving information about non-target U.S. persons. In the case of FBI queries intended to retrieve evidence of a crime, the interest in the retrieved information may be unrelated to national security. Consequently, the unjustified use of U.S.-person query terms to search the main repositories of unminimized Section 702 information presents “a serious risk of unwarranted intrusion into the private communications of . . . U.S. persons,” which “weighs substantially in the assessment of reasonableness.” October 18, 2018, Opinion at 89.

In contrast, UAM searches do not present remotely comparable Fourth Amendment concerns. UAM systems contain a limited amount of unminimized Section 702 information. If someone wanted to find and examine Section 702 information concerning a particular person, searching a UAM system would be a poor means of doing so. Searches that are conducted for a UAM purpose, moreover, will not generally be formulated in a way that is likely to retrieve unminimized communications of or concerning U.S. persons acquired under Section 702. It is possible to construct hypothetical counterexamples – e.g., a UAM search that is designed to

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 40

~~TOP SECRET//SI//ORCON//NOFORN~~

retrieve information about the system usage of a particular intelligence analyst during a particular time, and it is known that at such time the analyst was tracking a Section 702 target who communicates with U.S. persons. But even in such circumstances, any Fourth Amendment concerns are substantially allayed by the limited amount of Section 702 information subject to search on a UAM system, as well as the UAM purpose of the search, to which the substance of any retrieved Section 702 information will be generally irrelevant. (In the above hypothetical, the purpose of the UAM search is to retrieve information about the analyst's use of agency systems, not to retrieve or examine any Section 702 information.)

The Court accordingly will approve the proposed exclusion of UAM searches from the definition of "query" in the CIA, NSA, and FBI querying procedures and concomitant exemption of such searches from the requirements of those procedures. As explained above, however, that approval rests substantially on the factual premise that UAM searches are conducted against only a limited amount of unminimized Section 702 information that was incidentally copied during UAM processes. The validity of that premise could be affected by changes in the scope or functioning of the agencies' UAM activities. The Court, as a result, directs the government to update its descriptions of the UAM systems and processes employed by the FBI, CIA, and NSA by no later than March 26, 2021 – *i.e.*, two years from the government's prior UAM submissions.

**C. FBI Archival Systems**

The FBI maintains systems to archive copies of messages from its classified email and instant message systems. Like UAM systems, these archival systems are not main repositories of unminimized Section 702 information, but a limited amount of such information entered those

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

systems because FBI personnel included it in an email or instant message. As discussed below, the FBI's current minimization procedures prohibit the transmission of such information in emails or instant messages. The amount of such information in these archival systems consequently should be capped; otherwise, these systems present issues similar to those presented by UAM systems.

### 1. Background on Retention in FBI Archival Systems

The FBI's [REDACTED] maintains an archive of emails from [REDACTED] to assist in responding to discovery requests. See October 18, 2018, Opinion at 117. That system is also used for records management and processing of Freedom of Information Act requests and by the FBI's [REDACTED] investigative purposes. Id. [REDACTED] stores copies of messages from the FBI's [REDACTED] in a separate archival system. Id.

In 2018, the Court approved changes to the FBI's Section 702 minimization procedures for these archival systems. The first change prohibited the further placement of unminimized Section 702-acquired information in [REDACTED] Id. at 118, 120. The Court also approved the indefinite retention of such information that had already been placed in these archival systems, notwithstanding otherwise-applicable retention limits, subject to access to the systems being limited to "FBI personnel who require access to perform their official duties or assist in a lawful and authorized governmental function, including system administrators and other technical personnel, and who have received training on these minimization procedures and the Querying Procedures." Id. at 119-20. Such personnel can

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

access the archival systems only to assist in security, insider threat, inspection, and FBI internal-counterintelligence inquiries, functions, and investigations, and to respond to inquiries related to records management and discovery and can search those systems only to further such inquiries, functions, and investigations. *Id.* at 119. The Court also ordered that, in the event the FBI identified data in such an archival system as unminimized Section 702-acquired information and sought to retain it in that system, the government must state in its next quarterly report to the Court on Section 702 compliance matters: (1) whether the information could be retained on an FBI classified email or instant-messaging system as described in Sections III.F.4 or III.F.5 of the 2018 FBI Minimization Procedures or in connection with litigation matters as described in Section III.I.3 of those procedures; and (2) if not, the reason retention of the information in the archival system is necessary to the purposes served by that system. *Id.* at 138.

Finally, searches of the archival systems are currently subject to the FBI's querying procedures. *See* 2018 FBI Minimization Procedures § III.F.5 ("Because the classified e-mails in this archive may contain raw Section 702-acquired information, any queries in this archive must be conducted in accordance with the Querying Procedures."); *id.* § III.F.6 (same for instant-messaging archive).

## 2. Proposed Rules for Retention in Archival Systems

The proposed FBI minimization procedures treat retention of unminimized Section 702 information in these archival systems in the same manner as they treat retention of such information in UAM systems. If FBI personnel identify unminimized Section 702 information in one of these archival systems, they must remove it from the system unless (1) it meets generally

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

applicable retention criteria and is not otherwise subject to purge; or (2) “it is necessary to retain [it] for the purposes served by” the archival system in question, in which case the retention, and the reason therefor, must be included in the next quarterly report to the Court on Section 702 compliance matters, and the FBI must delete the information when it is no longer needed for such purpose. See 2019 FBI Minimization Procedures § III.F.5 and § III.F.6.

The proposed reporting requirement is narrower than the one that the Court adopted in October 2018, which requires reporting of every identified instance of continued retention of raw Section 702 data in an archival system, regardless of whether it is consistent with generally applicable retention criteria. On the merits that is a reasonable modification, particularly in view of the prohibition against putting such data in classified FBI emails and instant messages. For that reason, the Court approves the narrower reporting requirement on a prospective basis.

It must be noted, however, that the government has unjustifiably disregarded the current reporting requirement. Instead of taking concrete steps to comply even partially with the Court’s directive (or timely seeking relief from it), it chose to wait while the FBI reportedly worked on guidance to instruct its personnel on how to handle unminimized Section 702 information on these archival systems. See Letter Regarding the FBI’s Steps to Implement an Aspect of the Court’s 2018 Section 702 Opinion and Order, Sept. 27, 2019, at 3. In fact, it has taken so long to prepare this guidance that, instead of using it to instruct personnel on the October 2018 reporting requirement, which the government reports was the original plan, the FBI now intends to address only the narrower reporting requirement incorporated into the FBI’s proposed minimization

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

procedures. See Letter Regarding the FBI's Steps taken by the FBI to implement an aspect of the Court's 2018 Section 702 Opinion and Order, Nov. 20, 2019, at 4.

It should be unnecessary to state that government officials are not free to decide for themselves whether or to what extent they should comply with Court orders. The government has not sought retrospective relief from the reporting requirement imposed by the Court on October 18, 2018. Although the AG and DNI have amended the prior Section 702 certifications to authorize the FBI to apply its proposed minimization procedures to information acquired under prior certifications, that authorization only becomes "effective on October 17, 2019, or on the date upon which [this Court] issues an order concerning [the] amendments pursuant to subsection 702(j)(3) of the Act, whichever is later." [REDACTED]

[REDACTED] The Court's approval of those amendments does not have any nunc pro tunc effect, nor does it excuse the government from reporting instances of retention that it is already obligated to report. With respect to those instances of retention, the October 2018 reporting requirement remains in effect.

### 3. Proposed Rules for Searching Archival Systems

In another parallel with the proposed rules for UAM systems, the FBI's proposed querying procedures would exclude searches of these archival systems from the definition of "query" and therefore from the requirements of the querying procedures. Specifically, the definition of "query" in the FBI Querying Procedures exempts "searches conducted in the [archival] systems defined in Sections III.F.5 and 6 of the FBI's section 702 minimization procedures in furtherance of an authorized use specified in those provisions." 2019 FBI

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Querying Procedures § III.A. As noted above, those minimization provisions authorize searching such systems “to assist in security, insider threat, inspection, and FBI-internal counterintelligence inquiries, functions, and investigations, and to respond to inquiries related to records management and discovery.” 2019 FBI Minimization Procedures § III.F.5 and § III.F.6 (emphasis added). The underscored language describes purposes quite different from UAM purposes; however, it is also the case that searches in furtherance of records management and discovery, like UAM searches, will generally not be formulated to retrieve unminimized information about U.S. persons acquired under Section 702. In addition, the amount of unminimized Section 702 information in these archival systems is also limited, and, unlike UAM systems, there is no prospect of more such information being added to the archival systems. The Court concludes accordingly that the reasons for approving an equivalent exemption for searching UAM systems also apply to searches of these archival systems.

**D. NSA’s Retention Period for Upstream Collection Results**

The government proposes to increase the general retention period for information acquired by NSA’s upstream collection from two to five years. See 2019 NSA Minimization Procedures § 4(c)(2). NSA’s general retention period for results of downstream collection remains five years. Id. § 4(c)(1). The reasons for the historical distinction have been described in prior opinions, see, e.g., October 18, 2018, Opinion at 12-14, and are summarized here.

Internet transactions acquired by upstream collection before March 17, 2017, contained a greater proportion of information (including U.S.-person information) unrelated to 702 targets than other forms of 702 collection for several reasons. First, NSA sometimes acquired “multiple

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON/NOFORN~~

communication transactions,” or “MCTs,” through upstream collection. An MCT is a bundle of communications transiting part of the Internet together [REDACTED]

[REDACTED] containing multiple messages [REDACTED] See

Docket Nos. [REDACTED] Mem. Op. and Order, Apr. 26, 2017, at 15-16 (“April 26, 2017, Opinion”). (“Active user” refers to the user of a communication service to or from whom an MCT is in transit when it is acquired. Id. at 16.) Prior to March 17, 2017, NSA acquired MCTs without regard to whether the active user was a Section 702 target. Id. at 16-17. Moreover, NSA acquired communications, including MCTs, “about” – i.e., containing a reference to – a tasked selector, in addition to communications to or from a tasked selector. For example, if a single email message within an MCT contained a reference to a tasked email account, the entire MCT could be acquired, including numerous additional messages that did not contain a reference to, and were not to or from, the tasked account. Id. Those additional email messages could be wholly unrelated to the target. Id.

Because upstream collection prior to March 17, 2017, was more likely than other forms of Section 702 collection to acquire information concerning U.S. persons with no foreign intelligence value, heightened restrictions were placed on NSA’s retention, use, and dissemination of the results of upstream collection. One of those restrictions was a shorter, two-year retention period. See April 26, 2017, Opinion at 17-18, 26 n.29. As a result of compliance issues involving NSA’s failure to follow some of those heightened restrictions (specifically, a prohibition on U.S.-person queries), NSA [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

 Id. at 18-27. Specifically, that collection acquires MCTs only if a Section 702 target is the active user or – i.e., a sender or recipient of – the entire MCT, including each discrete communication contained within it. Id. at 26. NSA’s current minimization procedures now provide that “[a]ny communications acquired pursuant to section 702 that contain a reference to, but are not to or from, a person targeted in accordance with section 702 targeting procedures are unauthorized acquisitions and therefore will be destroyed upon recognition.” 2018 NSA Minimization Procedures § 4(c)(3) (emphasis added).

The NSA’s minimization procedures, as amended in March 2017 and approved in April 2017, required the sequestration and destruction of all upstream Internet transactions collected prior to March 17, 2017. See April 26, 2017, Opinion at 23-25. Aside from information retained subject to restricted access for litigation-hold purposes, NSA has completed its processes to destroy those transactions, see October 18, 2018, Opinion at 14; and any that might remain in NSA systems are subject to destruction upon recognition under the proposed NSA minimization procedures. See 2019 NSA Minimization Procedures § 4(c)(2).

In January 2018, Congress enacted the FISA Amendments Reauthorization Act of 2017 (“Reauthorization Act”), Pub. L. No. 115-118, 132 Stat. 3 (2018). The Reauthorization Act included Section 702(b)(5), which limits the acquisition of “abouts” communications – i.e., “communications that contain a reference to, but are not to or from, a target of an acquisition authorized” under Section 702(a). See Reauthorization Act § 103(a)(3). That provision imposes, with narrow exceptions for exigent circumstances, a requirement of congressional notification

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

and a 30-day congressional-review period before the government can resume abouts collection under Section 702. Id. § 103(b)(1)-(4).

In short, as of March 17, 2017, NSA eliminated the features of upstream collection that made it more likely than other forms of Section 702 collection to acquire non-target communications concerning U.S. persons and has purged Internet transactions acquired through upstream collection prior that date. The government contends that the results of upstream collection conducted after that date and currently possessed by NSA are no more sensitive, from a U.S.-person-privacy perspective, than the results of downstream collection, such that a five-year retention period is appropriate for both sets of data. The Court finds that approach reasonable. It is directing the government to provide prompt notice in the event that new types of selectors are tasked for upstream collection. See pages 81-82 infra. Such notification, together with the statutory pre-conditions to resuming acquisition of “abouts” communications, will permit the Court to examine whether future developments present a heightened risk to the privacy of U.S.-person information and warrant additional minimization protections.

**E. NSA’s Retention of Technical Information**

NSA’s current minimization procedures have special retention rules for “technical data base information,” which is defined as “information” – apparently of any type – that is “retained for cryptanalytic, traffic analytic, or signal exploitation purposes.” 2018 NSA Minimization Procedures § 3(j). What constitutes a cryptanalytic, traffic-analytic or signal-exploitation purpose is not further described. Under the current procedures, a five-year retention period generally applies to foreign communications of or concerning U.S. persons. Id. § 7(a). But NSA

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

may retain such communications “if necessary for the maintenance of technical data bases,” which the Court understands to mean necessary for one of the purposes identified above, as long as necessary “to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement,” which may be for longer than five years. Id. § 7(a)(1). And while NSA is generally required to destroy domestic communications promptly upon recognition, id. § 6, they may be retained as long as necessary “to allow a thorough exploitation and to permit access to data that is, or is reasonably believed likely to become, relevant to a current or future foreign intelligence requirement,” provided that the Director, Operations Directorate, NSA makes a specific written determination that the communications are “reasonably believed to contain technical data base information” and that the sender or intended recipient of the communications was properly targeted under Section 702. Id. § 6(3). (A foreign communication is “a communication that has at least one communicant outside of the United States”; all other communications are domestic communications. Id. § 3(e).)

The government reports:

NSA undertook an examination of its holdings and determined that the only information which it is potentially currently retaining as “technical data base information” is information that is encrypted or reasonably believed to contain secret meaning, or technical information (e.g., encryption algorithms, keys, credential records) that has previously been addressed in various compliance notices and updates to the Court regarding NSA’s modernization of its cryptographic systems. As described previously to the Court, such technical information does not include the underlying communications originally containing such information.

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 50

~~TOP SECRET//SI//ORCON//NOFORN~~

September 17, 2019, Memorandum, at 30 (footnote omitted). Accordingly, the proposed NSA procedures dispense with the term “technical data base information” and include narrower retention provisions for information needed for decryption and decipherment efforts.

With regard to foreign communications of or concerning United States persons, NSA may retain information “that reasonably appears to be encrypted or to contain secret meaning for a sufficient duration to permit exploitation.” 2019 NSA Minimization Procedures § 7(a)(1)a. Once the information is decrypted or deciphered, the general five-year retention period is calculated “from the date of decryption or decipher.” *Id.* NSA may also retain “technical information (e.g. encryption algorithms, keys, credentials) contained in, or derived from,” such communications “for any period of time during which such information is used for cryptanalysis or processing information into intelligible form.” *Id.* § 7(a). Technical information to be retained under this provision “does not include the underlying communications” from which the technical information was derived. *See* September 17, 2019, Memorandum, at 30. It is possible that such technical information could be used for other purposes.

provided that

any use or dissemination of such information is “in accordance with the requirements in these procedures.” 2019 NSA Minimization Procedures § 7(a).

With regard to domestic communications, the proposed procedures do not include any provisions for exempting information from the generally applicable requirement to destroy such communications upon recognition because it is useful in decryption and decipherment efforts. *See* September 17, 2019, Memorandum, at 32.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Because these new provisions clarify and narrow the circumstances in which NSA may retain information for certain purposes, they present no difficulty in finding that the proposed NSA minimization procedures comport with statutory and Fourth Amendment requirements.

**F. NSA's Retention of Information Regarding Communications-Security Vulnerabilities**

The current procedures provide that NSA may retain a domestic communication, notwithstanding the prompt-destruction requirement that generally applies to such communications, if the Director of NSA makes a specific written determination that the sender or intended recipient of the communication was properly targeted and the communication is “necessary to understand or assess a communications security vulnerability.” 2018 NSA Minimization Procedures § 6(3). The proposed procedures clarify that the communications-security vulnerability must be “of a United States Government or National Security system” and that the domestic communication and, if applicable, the transaction in which it is contained may be retained while the information “is of use in identifying or defending against such a vulnerability.” 2019 NSA Minimization Procedures § 6(3). NSA may also disseminate the information to the FBI or other parts of the U.S. government. The Court understands that disseminations under this provision must be for the same purpose, and with that understanding, it finds the revised provision to be reasonable.

**G. NCTC Procedures Regarding Automated Translation Assistance from CIA**

The current NCTC minimization procedures permit NCTC to provide unminimized information to another federal agency when, “because of [its] technical or linguistic content, [such information] may require further analysis” by the recipient agency “to assist NCTC in

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

determining [its] meaning or significance.” 2018 NCTC Minimization Procedures § D.5. Strict controls apply to how the recipient agency handles the information, including that:

(1) disclosure is made “only to those personnel within assisting federal agencies involved in the translation or analysis” of the disclosed information, the number of such personnel is “restricted to the extent reasonably feasible,” and the information is not further disclosed within the recipient agency, id. § D.5.b; and

(2) upon the conclusion of assistance, all copies of the information in question “will either be returned to NCTC or be destroyed, with an accounting of such destruction made to NCTC,” id. § D.5.d.

(The FBI and CIA’s minimization procedures for Section 702 information have similar provisions. See 2018 FBI Minimization Procedures § IV.D; 2018 CIA Minimization Procedures § 7.b; see also 2018 NSA Minimization Procedures § 9(b) (similar restrictions regarding technical or linguistic assistance from foreign governments).)

In a notice filed on June 26, 2019, the government disclosed that the CIA’s provision of assistance to NCTC by use of [REDACTED] does not comport with those restrictions. See Preliminary Notice of Compliance Incident Regarding Data Acquired Pursuant to the FISA, June 26, 2019 (“June 26, 2019 Notice”). Specifically [REDACTED] designedly “creates and retains logs for up to five years that contain encrypted source text,” which “may include the raw product being translated [REDACTED] Id. at 2 & n.3. The notice reported that “only CIA [REDACTED] technical personnel, [REDACTED] [REDACTED], currently have access to data [REDACTED] Id. at 3.

(The current and proposed CIA minimization procedures define “CIA personnel” to include “any employees of CIA and any other personnel acting under the direction, authority, or control of the Director of the CIA.” 2018 CIA Minimization Procedures § 1.c; 2019 CIA Minimization

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Procedures § 1.c.) The government further represented that “NCTC has no other means to translate data.” June 26, 2019, Notice at 3.

Section D.5.f of the proposed NCTC minimization procedures would authorize CIA “to maintain records of raw section 702-acquired information disclosed by NCTC to CIA for linguistic assistance and stored [REDACTED] for a period of five years from the date of receipt,” with access to such records “restricted to CIA technical personnel responsible for the maintenance and operation [REDACTED] 2019 NCTC Minimization Procedures § D.5.f. Relying on that access restriction and the government’s representations, the Court concludes that the five-year retention period does not preclude a finding that the proposed NCTC minimization procedures satisfy the definition of “minimization procedures.” It views Section D.5.f as a narrow exception to the general rule that agencies providing technical or linguistic assistance should not retain unminimized data after that assistance has been completed. If the government seeks additional exceptions, the Court expects to scrutinize closely the need for longer retention in other contexts.

#### **H. Other Provisions**

The Court has examined the following provisions, as revised in the proposed minimization procedures, and concludes that they are consistent with finding that the proposed procedures satisfy the applicable definition of “minimization procedures.”

##### **1. Retention of U.S.-Person Information by the CIA**

Under both its current and proposed minimization procedures, the CIA may generally retain unminimized information that may contain U.S.-person information for five years. See 2018 CIA Minimization Procedures § 2.a; 2019 CIA Minimization Procedures § 2.a. U.S.-

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

person information may be retained beyond that period if it meets stated retention criteria, subject to a requirement to delete U.S.-person identities, unless such identity “is necessary, or it is reasonably believed that it may become necessary, to understand or assess the information.”

2018 CIA Minimization Procedures § 3; 2019 CIA Minimization Procedures § 3. Section 3 of the proposed procedures is revised to omit reference to “outside of access-controlled repositories,” 2018 CIA Minimization Procedures § 3, so that its retention requirements unambiguously apply to retention in any form. The government advises that the revisions are also intended to clarify that those requirements apply “to both the communication of a United States person and information concerning a United States person in any communication.” September 17, 2019, Memorandum, at 32-33.

## 2. Court Notification Requirements

Each agency’s minimization procedures contain provisions under which a high-level official, upon making a specified determination, can approve actions that contravene otherwise-applicable minimization requirements, such as retaining information that otherwise would have to be destroyed. In the proposed procedures, a number of such provisions have been revised to require the government to report such approvals to the Court. See 2019 NSA Minimization Procedures § 6 (retention and handling of domestic communications); id. § 7(a)(1) (retention of foreign communications of or concerning United States persons beyond five years); 2019 FBI Minimization Procedures § III.D.4.b (retention of unreviewed information in electronic and data storage systems beyond five years); id. § III.E.4.c (retention of information that does not otherwise meet the standard for retention in ad hoc storage systems beyond five years); 2019 CIA

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Minimization Procedures § 2.a (retention of information that does not otherwise meet the standards for retention beyond five years); 2019 NCTC Minimization Procedures § B.2.a (retention of unreviewed information beyond five years). Such reporting should better enable the Court to ensure that the agencies are implementing those provisions reasonably.

### 3. Loss or Abandonment of Lawful Permanent Resident Status

A lawful permanent resident (LPR) of the United States is a U.S. person for purposes of Section 702. See 50 U.S.C. §§ 1801(i), 1881a(a). The NSA, FBI, NCTC, and CIA minimization procedures now provide that a determination that a person has lost or abandoned LPR status, and therefore is no longer a U.S. person, may be made in one of two ways: (a) in consultation with the agency's Office of General Counsel and based on either a court order revoking the person's U.S. person status or an official abandonment of LPR status executed by the person and filed with the U.S. Customs Citizenship and Immigration Services; or (b) in consultation with the agency's OGC and the National Security Division of the Department of Justice. See 2019 NSA Minimization Procedures § 3(j)(3); 2019 FBI Minimization Procedures § I.D; 2019 NCTC Minimization Procedures § A.4.c; 2019 CIA Minimization Procedures § 1.d(3). Parallel changes are made to the agencies' respective querying procedures, see 2019 NSA Querying Procedures § III.B.3; 2019 FBI Querying Procedures § III.B.3; 2019 CIA Querying Procedures § III.B.3; 2019 NCTC Querying Procedures § III.B.3, and the NSA's targeting procedures, see 2019 NSA Targeting Procedures § I at 4. The Court regards these changes as an improvement because they require an appropriate level of scrutiny for these consequential determinations.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

## I. Conclusion

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that, as written, the proposed minimization procedures for the FBI, NSA, CIA, and NCTC, in conjunction with the querying procedures for those agencies, satisfy the definition of minimization procedures at 50 U.S.C. § 1801(h); and that those querying procedures satisfy the requirements of Section 702(f)(1).

## V. **FOURTH AMENDMENT REQUIREMENTS**

The Court must also assess whether the proposed targeting, minimization, and querying procedures are consistent with the requirements of the Fourth Amendment. See § 702(j)(3)(A).

That Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

“The touchstone of the Fourth Amendment is reasonableness.” In re Certified Question of Law, 858 F.3d 591, 604 (FISA Ct. Rev. 2016) (per curiam) (“In re Certified Question”).

Although “[t]he warrant requirement is generally a tolerable proxy for ‘reasonableness’ when the government is seeking to unearth evidence of criminal wrongdoing, . . . it fails properly to balance the interests at stake when the government is instead seeking to preserve and protect the nation’s security from foreign threat.” Id. at 593. A warrant is not required therefore to conduct surveillance “to obtain foreign intelligence for national security purposes . . . directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

States.” In re Directives Pursuant to Section 105B of FISA, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (“In re Directives”). The FISC has repeatedly reached the same conclusion regarding Section 702 acquisitions. See, e.g., Docket Nos. [REDACTED] Mem. Op. and Order, Nov. 6, 2015, at 36-37 (“November 6, 2015, Opinion”); September 4, 2008, Opinion at 34-36.

In prior reviews of Section 702 procedures, the Court has assessed the reasonableness of the government’s procedures as a whole. See, e.g., November 6, 2015, Opinion at 39 (assessing “the combined effect” of the targeting and minimization procedures ); October 18, 2018, Opinion at 85-88 (declining invitation of amici curiae to conduct Fourth Amendment evaluation of querying practices in isolation ). Restrictions on how the government targets acquisitions under Section 702 and how it handles information post-acquisition limit the degree of intrusion on individual privacy interests protected by the Fourth Amendment. For reasons explained above, the Court has found that the proposed targeting procedures, as written, are reasonably designed to limit acquisitions to targeted persons reasonably believed to be non-United States persons located outside the United States. The Fourth Amendment does not protect the privacy interests of such persons. See, e.g., November 6, 2015, Opinion at 38; September 4, 2008, Opinion at 37 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)).

To the extent U.S.-person information is acquired under Section 702 – e.g., when a communication between a U.S. person and a Section 702 target is intercepted – the government can reduce the intrusiveness of the acquisition for Fourth Amendment purposes by restricting use or disclosure of such information. See In re Certified Question at 609. The FISC has previously

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

found that “earlier versions of the various agencies’ targeting and minimization procedures adequately protected the substantial Fourth Amendment interests that are implicated by the acquisition of communications of such United States persons.” November 6, 2015, Opinion at 38-39 (citing Docket Nos. [REDACTED] Mem. Op. and Order, August 26, 2014 (“August 26, 2014, Opinion”); Docket Nos. [REDACTED] and [REDACTED] Mem. Op., Aug. 30, 2013, at 6-11 (“August 30, 2013, Opinion”)). Specifically, “the combined effect of these procedures” was “to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated’ and to ensure that ‘non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary.’” November 6, 2015, Opinion at 39 (citing August 26, 2014, Opinion at 40).

The Court takes all of these factors into account in assessing the reasonableness of the procedures under the Fourth Amendment. Under the applicable totality-of-circumstances approach, it must balance “the degree to which [governmental action] intrudes upon an individual’s privacy” against “the degree to which it is needed for the promotion of legitimate governmental interests.” In re Certified Question, 858 F.3d at 604-05 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)). “The more important the government’s interest, the greater the intrusion that may be constitutionally tolerated.” In re Directives, 551 F.3d at 1012.

The Court regards the privacy interests at stake in Section 702 acquisition as substantial. The government tasks a large number of selectors used by non-U.S. persons for acquisition under Section 702. See, e.g., DNI Statistical Transparency Report Regarding Use of National Security

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Authorities (April 2019), at 13 (reporting an estimated amount of over 164,000 Section 702 targets in 2018). Although not separately quantified, there is presumably a substantial amount of information of or concerning United States persons acquired under Section 702, as described above.

On the other side of the constitutional balance, acquiring “foreign intelligence with an eye toward safeguarding the nation’s security serves . . . a particularly intense interest.” In re Certified Question, 858 F.3d at 606 (internal quotation marks omitted). For that reason, the FISC has observed that “the government’s investigative interest in cases arising under FISA is at the highest level and weighs heavily in the constitutional balancing process.” Id. at 608.

Measures to protect individual privacy can be decisive in the proper balancing of these interests:

If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the government’s actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

In re Directives, 551 F.3d at 1012.

In this case, the Court has carefully considered how the proposed procedures seek to protect private U.S.-person information from misuse.

The Court concludes that, in combination, the proposed targeting, minimization, and querying procedures will adequately guard against error and abuse, taking into account the individual and governmental interests at stake. It therefore finds that those procedures, as

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 60

~~TOP SECRET//SI//ORCON//NOFORN~~

written, are consistent with the requirements of the Fourth Amendment. The Court next considers questions of implementation.

## VI. IMPLEMENTATION AND COMPLIANCE ISSUES

FISC review of the sufficiency of Section 702 procedures is not limited to the procedures as written, but also encompasses how they are implemented. See, e.g., October 18, 2018, Opinion at 68. It is appropriate, accordingly, to examine significant issues regarding such implementation.

### A. FBI Querying Issues

FBI querying practices raise significant questions regarding (1) recordkeeping and documentation requirements for use of U.S.-person query terms; (2) the substantive standard for conducting queries; and (3) queries that are designed to retrieve or in fact retrieve evidence of a crime that is not foreign-intelligence information.

#### 1. **Recordkeeping and Documentation Requirements for U.S.-Person Query Terms**

Recordkeeping and documentation requirements for the FBI's use of U.S.-person query terms have been extensively considered in prior proceedings, as briefly summarized below.

In October 2018, the Court found two deficiencies regarding the FBI's procedures as then proposed:

(1) the querying procedures were inconsistent with Section 702(f)(1)(B) because they did not require the FBI to keep records that identify which terms used to query unminimized Section 702 information are United States-person query terms, see October 18, 2018, Opinion at 52-62, 133; and

(2) the minimization procedures and querying procedures were inconsistent with the requirements of Section 702(e) and Section 702(f)(1)(A), respectively, and also with

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Fourth Amendment requirements, because they did not require adequate documentation of the justifications for queries that use United States-person query terms. Id. at 133-34.

The second finding of deficiency rested substantially on the prevalence of queries that did not meet the substantive standard for the FBI to query unminimized Section 702 information. The Bureau's procedures authorized such queries if they were reasonably likely to return foreign-intelligence information or evidence of a crime. Id. at 66-67. In practice, however, the FBI conducted a large number of suspicionless queries that did not meet that standard, some of which involved a large number of U.S.-person query terms. Id. at 68-72.

Upon appeal by the government, the FISCR affirmed this Court's finding that the querying procedures were inconsistent with the recordkeeping requirement of Section 702(f)(1)(B). See In re DNI/AG Certifications at 4-5, 22-38, 42-43. The FISCR did not decide whether the FBI's procedures were deficient for the second reason identified by the FISC. See id. at 38, 43.

In response to the FISCR's affirmance, the government amended the FBI's querying procedures. This Court approved those amendments on September 4, 2019. See Docket Nos. [REDACTED] Mem. Op. and Order, Sept. 4, 2019, at 16-17

("September 4, 2019, Opinion"). The amended querying procedures require the FBI:

- (1) to keep records that identify which terms used to query unminimized Section 702 information are U.S.-person query terms, id. at 7-8, and
- (2) to document in writing why a query involving a U.S.-person query term satisfies the querying standard before accessing the contents of communications retrieved by the query (except for queries that are subject to Section 702(f)(2), which is discussed at pages 69-73 infra.). Id. at 8-9. (This documentation requirement adopts a recommendation made by amici curiae. See October 18, 2018, Opinion at 92-93, 96-97.)

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

In this Opinion, the term “contents” refers to any information concerning the substance, purport or meaning of a communication. See § 702(f)(3)(A); 18 U.S.C. § 2510(8). In its October 18, 2018, Opinion, the Court directed the government “to describe the types of information acquired by the FBI under Section 702 that the government regards as [non-contents] metadata.” October 18, 2018, Opinion at 114. The government’s response described, among other things, the FBI’s current practices of treating certain [REDACTED] as contents information. See Gov’t Response to the Court’s Oct. 18, 2018, Order and Motion for Extension of Time, Feb. 1, 2019, at 10-18. The Court’s approval of the FBI’s querying and minimization procedures relies on those descriptions, and the Court expects the FBI to implement those procedures in accordance with them.

When it submitted the amended procedures, the government reported that the FBI could not immediately comply with the new recordkeeping and documentation requirements and proposed a timetable for their full implementation, including the requisite training of FBI personnel. See September 4, 2019, Opinion at 10-16. For the systems primarily used by the FBI to query unminimized Section 702-acquired information – [REDACTED] – the FBI expected to have completed necessary training and systems modifications, which will support the generation of the required records, by mid-December 2019. Id. at 13-14. The government also reported that the FBI conducts some queries of unminimized Section 702 information on a system [REDACTED]. The government was considering whether to attempt systems modifications for [REDACTED] which were expected to be costly and time consuming; in the meantime [REDACTED] users are required to keep

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

written records of U.S.-person query terms and the justification for queries, to the extent required by the amended procedures. Id. at 11. Finally, the FBI planned to retain and query certain forms of unminimized Section 702 information on a system [REDACTED]. If it determines that it cannot arrange [REDACTED] to generate the required records automatically, its personnel will be required to create written records, as with [REDACTED]. Id. 15-16. (As of November 8, 2019, the FBI still was not storing unminimized Section 702 information [REDACTED] 45-Day Report Regarding the FBI's Implementation of the FBI's Section 702 Querying Procedures, Nov. 8, 2019, at 2 n.1. ("45-Day Report, November 8, 2019").)

The Court found that the government's plans for full implementation did not preclude approval of the procedures and ordered periodic reporting on their implementation. See September 4, 2019, Opinion at 14-15, 17. The government has filed two such reports. See 45-Day Report Regarding the FBI's Implementation of the FBI's Section 702 Querying Procedures, Sept. 26, 2019 ("45-Day Report, September 26, 2019") and 45-Day Report, November 8, 2019. They advise that the training efforts, as well as the systems modifications for [REDACTED] are on schedule. When FBI personnel seek to run a query of unminimized Section 702 information on the modified systems, they will first be required to state whether the query involves a U.S.-person or presumed U.S.-person query term. If it does, they must record why it meets the querying standard before they can access any Section 702-acquired contents returned by the query. See 45-Day Report, September 26, 2019, at 9-13. All query terms and justifications will be logged for auditing purposes. Id. at 11, 14.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Personnel who query unminimized Section 702 information on [REDACTED] are provided with a link to an internal FBI SharePoint site to record whether a query involves a U.S.-person or presumed U.S.-person query term. If so, they too must document why the query satisfies the querying standard before viewing any contents returned by the query. *Id.* at 15. In view of “the time and anticipated cost” of modifying [REDACTED] to generate and store the required records, the FBI continues to deliberate about whether “to maintain the SharePoint site . . . as a long-term solution for [REDACTED].” *See* 45-Day Report, November 8, 2019, at 16-17.

Users who query unminimized Section 702 information on an ad hoc system are required to provide the required documentation on the same SharePoint site. *See* 45-Day Report, September 26, 2019, at 17-18. (FBI personnel may work with unminimized Section 702 information on an “ad hoc system” only if “they cannot fully, completely, efficiently, or securely review or analyze [such] information in an electronic and data storage system,” such as [REDACTED].” *See* 2019 FBI Minimization Procedures § III.E.1. at 23. Unminimized Section 702 information on ad hoc systems is subject to special access restrictions. *Id.* § III.E.3.a. at 24.)

In sum, the FBI is hewing to the previously described implementation schedule.

## 2. Violations of the Querying Standard

It must be noted, however, that there still appear to be widespread violations of the querying standard by the FBI. For example, NSD’s oversight review of the Bureau’s [REDACTED] [REDACTED] in June 2019 revealed queries of unminimized Section 702 information that were not reasonably likely to retrieve foreign-intelligence information or evidence of crime, including:

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

- queries to vet a potential source;
- queries to vet a candidate to become a local police officer; and
- queries to find information related to a planned visit [REDACTED] by foreign government officials.

Notice of compliance incidents regarding the FBI's [REDACTED] querying of raw FISA-acquired information, Sept. 18, 2019, at 2-3.

In July 2019, an oversight review of [REDACTED] discovered 87 queries of raw FISA-acquired information in [REDACTED] that were not reasonably likely to retrieve foreign-intelligence information or evidence of a crime, including:

- queries of college students participating in a "Collegiate Academy"; and
- queries of individuals who had visited the FBI office (e.g., for maintenance).

Notice of compliance incidents regarding the FBI's [REDACTED] querying of raw FISA-acquired information, Sept. 6, 2019, at 1-2.

Additional improper queries include:

- [REDACTED] conducted queries to vet potential sources and to get information about a victim complainant, and conducted other overly broad queries (e.g., using the terms [REDACTED])
- [REDACTED] conducted queries using a complainant's identifying data;
- [REDACTED] conducted queries using identifiers of individuals applying to work on [REDACTED] and other overbroad terms such as [REDACTED]
- [REDACTED] conducted queries using identifiers of police officer candidates.

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Quarterly Report to the FISC Concerning Compliance Matters Under Section 702, Sept. 20, 2019 (“September 2019 Quarterly Report”), at 115-117, 119-122.

Most recently, the government has reported that, in August 2019, [REDACTED] [REDACTED] query unminimized Section 702 information using the identifiers for approximately 16,000 persons who [REDACTED]. See Preliminary Notice of compliance incidents regarding the FBI’s [REDACTED] querying of raw FISA-acquired information, Nov. 25, 2019, at 2. NSD assesses that the queries for seven of those persons satisfied the querying standard because of their ties to a [REDACTED] investigation, but all the other queries did not. Id. at 3. The FBI maintains that the queries for all 16,000 persons were reasonably likely to return foreign-intelligence information or evidence of a crime because [REDACTED]

[REDACTED] Id. at 2-3. These queries are similar to indiscriminate queries that the FBI previously conducted for persons with access [REDACTED]. Id. at 3. “NSD has asked FBI to determine whether similar queries have been conducted by other field offices”; if so, they will be reported to the Court. Id.

Based on the facts reported, the FBI’s position that the queries for all 16,000 persons were reasonably likely to retrieve foreign-intelligence information or evidence of a crime is unsupportable. Apart from the seven individuals referenced above, there was no indication that [REDACTED] was involved in criminal activity or foreign intelligence-related conduct, or any other reason to believe that running queries using identifiers for [REDACTED] would return [REDACTED]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

foreign-intelligence information or evidence of a crime. There is no relevant distinction between [REDACTED] queries and other broad, suspicionless queries previously identified by the government and the Court as violations of the querying standard. See October 18, 2018, Opinion at 68-69.

The Court has previously assessed that requiring FBI personnel to document why a query involving a U.S.-person query term is reasonably likely to have returned foreign-intelligence information or evidence of crime before examining contents returned by the query should “help ensure that FBI personnel . . . have thought about the querying standard and articulated why they believe it has been met” and prompt them “to recall and apply the guidance and training they have received on the querying standard.” See id. at 93; see also In re DNI/AG Certifications at 41 (that requirement may “motivate FBI personnel to carefully consider . . . whether a query satisfies” the standard). The recently reported querying violations suggest that some FBI personnel still need such help. That is not altogether surprising. As discussed above, the FBI is really just starting to implement that documentation requirement on a comprehensive basis. For that reason, the improper queries described above do not undermine the Court’s prior determination that, with that requirement, the FBI’s querying and minimization procedures meet statutory and Fourth Amendment requirements.

A number of violations apparently result, moreover, from the failure of FBI personnel to opt out of querying raw FISA-acquired information when they did not intend to query it. See, e.g., Notice of compliance incidents regarding the FBI’s [REDACTED] querying of raw FISA-acquired information, Nov. 14, 2019, at 2; Notice of compliance incidents regarding the

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

FBI's [REDACTED] querying of raw FISA-acquired information, Oct. 11, 2019, at 2. The government reports that, as a remedy, the FBI is modifying [REDACTED] to make it easier to opt out of searching Section 702 information before conducting a query. See 45-Day Report, November 8, 2019, at 2-3. Such modifications provide additional reason to expect improvement in the FBI's compliance with the querying standard.

### 3. Evidence-of-Crime Queries

Section 702(f)(2)(A) requires the FBI (not other agencies) in specified circumstances to obtain a FISC order before accessing the contents of unminimized Section 702 information. Specifically, that requirement applies only to contents retrieved by a query involving a U.S.-person query term, where the query is made “in connection with a predicated criminal investigation . . . that does not relate to the national security” and is “not designed to find and extract foreign intelligence information.” Id. To issue such an order, a FISC judge must find probable cause to believe that the contents in question would provide evidence of criminal activity, contraband or the fruits or instrumentalities of crime. See Section 702(f)(2)(C)(ii), (D). The FBI need not obtain a Court order if it “determines there is a reasonable belief” that the contents sought “could assist in mitigating or eliminating a threat to life or serious bodily harm.” Section 702(f)(2)(E).

The government has never applied to the FISC for an order under Section 702(f)(2), but FBI personnel have violated Section 702(f)(2) by accessing Section 702-acquired contents returned by a query under circumstances in which they were required to first obtain such an order. Some violations resulted in part from the manner in which FBI systems displayed

~~TOP SECRET//SI//ORCON//NOFORN~~

information in response to queries. For example, [REDACTED] displayed query results in a summary field that showed 100 characters of text around the query term within the records identified as responsive to the query. See Preliminary notice of compliance incidents and of potential compliance incidents regarding FBI queries of unminimized Section 702-acquired information designed to return evidence of a crime unrelated to foreign intelligence, Sept. 13, 2019, at 4. In some cases, moreover, FBI personnel are known to have taken further steps in response to such displays (e.g., opening “products” containing contents returned by a query), thereby accessing Section 702-acquired contents beyond what was initially displayed to them. Id. at 3.

The reported violations were discovered during oversight reviews at four FBI field offices. Id. at 2-3; Notice of compliance incidents regarding the FBI’s querying of raw FISA-acquired information, Sept. 17, 2019, at 1-2. Given how the manner in which FBI systems displayed query results contributed to the reported violations, it is likely that similar violations of Section 702(f)(2) have occurred across the Bureau. It is therefore important that the systems modifications to [REDACTED] are also designed to facilitate compliance with Section 702(f)(2). Users of those systems who state that a query involves a U.S.-person or presumed U.S.-person query term will be required to state whether the query is being conducted in connection with a predicated criminal investigation that is unrelated to national security. If so, the system will prevent access to responsive Section 702-acquired contents unless the user states that either a FISC order has been obtained or the contents could assist in mitigating or eliminating a threat to life or serious bodily harm such that an order is not required under Section 702(f)(2)(E). See 45-Day Report, September 26, 2019, at 10, 13-14. [REDACTED] receive a

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 70

~~TOP SECRET//SI//ORCON//NOFORN~~

reminder of the requirements for evidence-of-crime queries and have the ability to “modify their profile so that 702 content is hidden from their results.” Request for relief from requirement to report instances in which FBI personnel receive and review Section 702-acquired information concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information, Oct. 4, 2019, at 7 (“October 4, 2019, Request”). Ongoing training efforts also focus on compliance with Section 702(f)(2). *Id.* at 9 n.6; see also 45-Day Report, November 8, 2019, at 4-5 (FBI users required to complete mandatory training via FBI’s Virtual Academy by December 13, 2019).

In view of the government’s efforts to improve compliance with Section 702(f)(2), the Court is prepared to approve the FBI’s querying procedures. It intends, however, to monitor compliance with Section 702(f)(2) closely.

Relatedly, the government seeks relief from a reporting requirement that has been in effect since November 2015. The October 18, 2018, Opinion carried it forward as follows:

The government shall promptly submit in writing a report concerning each instance in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign-intelligence information. The report should include a detailed description of the information at issue and the manner in which it has been or will be used for analytical, investigative, or evidentiary purposes. It shall also identify the query terms used to elicit the information and provide the FBI’s basis for concluding that the query was consistent with applicable minimization procedures. The government need not file such a report for a query for which it files an application with the FISC pursuant to Section 702(f)(2).

October 18, 2018, Opinion at 136. This reporting requirement was first imposed because a prior FISC opinion relied on the government’s representation that “queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results from the

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Section 702-acquired data,” and the Court sought reassurance that its “risk assessment is valid.” November 6, 2015, Opinion at 44.

The government has not reported such instances in timely fashion. Rather, they have been reported to the Court belatedly, usually after they were uncovered during oversight reviews. The government now seeks relief from this reporting requirement “because the requirements in Section 702(f)(2) are a sufficient mechanism for the Court to assess the risk that the results of a query designed to elicit evidence of crimes unrelated to foreign intelligence will be viewed or otherwise used in connection with an investigation that is unrelated to national security.” October 4, 2019, Request at 8. But it would be premature to regard the government’s implementation of Section 702(f)(2) as a sufficient source of information. As discussed above, the FBI has repeatedly accessed Section 702-acquired contents under circumstances requiring a FISC order under Section 702(f)(2), but has never applied for such an order.

Closer to the mark is the government’s contention that implementing both Section 702(f)(2) and the November 2015 reporting requirement could complicate training and systems design. See October 4, 2019, Request at 8-9. For example, Section 702(f)(2) looks to whether a query involves a U.S.-person query term, while the applicability of the November 2015 reporting requirement depends on whether U.S.-person information is retrieved. And Section 702(f)(2) is implicated only when contents are accessed, while the November 2015 reporting requirement does not distinguish between contents and non-contents information.

The Court has decided to retain a reporting requirement separate from Section 702(f)(2) because the obligation to get a FISC order under that section is limited to queries conducted in

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

the context of a predicated criminal investigation. The FBI conducts numerous queries of Section 702 information at earlier investigative stages. See October 18, 2018, Opinion at 75. Reports about queries at those stages remain relevant to the Court's interest in receiving information about the extent to which U.S.-person privacy interests are implicated by queries that are not designed to find and extract foreign-intelligence information. The Court has concluded, however, that it is appropriate to modify the prior reporting requirement so that it will focus on the use of U.S.-person query terms, rather than on whether U.S.-person information is accessed as a result of a query, and will be triggered only when contents information is accessed. Such modifications should make it considerably simpler for the government to implement the requirement in combination with Section 702(f)(2), while still requiring reporting in situations where Fourth Amendment concerns are likely to be implicated. See October 18, 2018, Opinion at 93 (queries that use U.S.-person query terms and result in review of contents are "the subset of queries that are particularly likely to result in significant intrusion into U.S. persons' privacy").

**B. NSA Querying Issues**

NSA's procedures require that every query "must be reasonably likely to retrieve foreign intelligence information." 2018 NSA Querying Procedures § IV.A. In a Notice filed on October 10, 2019, the government reported that, in November 2018, NSA ran a series of queries using U.S.-person identifiers associated with

Notice of Compliance Incident regarding Section 702 Metadata

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Queries Conducted by the NSA, Oct. 10, 2019, at 2 (“October 10, 2019, Notice”). NSD, after reviewing these queries as apart of routine oversight, reported:

Although the NSA analysts who ran the queries were searching for possible connections between [REDACTED] and international terrorist organizations, due to the attenuation between [REDACTED] queried, [REDACTED] and the foreign intelligence information sought, the November 2018 metadata queries were not reasonably likely to retrieve foreign intelligence information and did not meet the requirements of the NSA Querying Procedures.

Id. at 3. In a separate incident that was reported by the analyst involved, NSA queried Section 702-acquired content information using twenty-three U.S.-person identifiers that were determined not to meet the querying standard because they were too attenuated from the foreign intelligence they were intended to return. See Notice of Compliance Incidents Regarding Improper Queries, Nov. 13, 2019, at 2. The queries did not return any FISA results. Id. In both cases, the personnel involved received instruction on Section 702 querying requirements. Id.; October 10, 2019, Notice at 3. The Court will continue to monitor closely the manner in which U.S.-person identifiers are used by all relevant agencies to query Section 702-acquired information.

**C. Failure to Purge Recalled Reports**

The government has reported incidents of non-compliance resulting from NCTC’s failure to purge its copies of NSA reports, which NSA had recalled for FISA-compliance reasons. See Preliminary Notice of Compliance Incident Regarding Incomplete Purges of Data Acquired Pursuant to the FISA, March 13, 2019; Supplemental Notice of Compliance Incident Regarding Incomplete Purges of Data Acquired Pursuant to the FISA, September 17, 2019 (“September 17, 2019, Supplemental Notice”). NCTC eventually deleted [REDACTED] recalled reports that contained FISA-

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

acquired information, but it did not know whether all [REDACTED] reports were recalled for FISA compliance-related reasons. See September 17, 2019, Supplemental Notice, at 2. Intelligence Community (IC) agencies sometimes recall reports for reasons unrelated to FISA compliance – e.g., inaccurate information included in the report, changed analysis, or typographical mistakes. See id.

In July 2019, ODNI sent a data call to the IC “to identify if other agencies are similarly impacted by this issue and how each agency handles recalled and revised NSA reports.” Id. Pending the results of the data call, the government ceased all remedial measures with respect to NCTC systems. Id. By order dated October 3, 2019, the Court directed the government to provide the results of the ODNI data call and describe how each IC agency is handling any improperly retained reports or, if the results of the ODNI data call are pending at the time of submission, to provide updated information and a proposed timetable for completion. See Order, Oct. 3, 2019, at 3. The government’s responsive submission outlined IC policy on revising or recalling intelligence products and assessed that the CIA, NSA, and NCTC may be retaining copies of reports which had been recalled for FISA compliance reasons. See [Corrected] Report in Response to the Court’s Order Dated October 3, 2019, Nov. 13, 2019, at 8. Specifically, recalled reports can still be viewed on some NCTC systems, NSA does not delete recalled reports from all of its data stores, and the CIA does not purge recalled reports from its systems because the recall does not specify whether the report contains information subject to purge. Id. at 5-8.

The government describes as “[o]ne potential solution” a requirement for “issuing agencies to specifically identify when reports are recalled due to FISA compliance reasons,”

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

which reportedly would require the DNI “to revise current policy.” *Id.* at 8. Although “ODNI and the IC agencies are exploring possible changes to the reports recall process that would involve a change in policy, . . . there is no estimated timeline for resolution of this matter.” *Id.* at 8-9.

The agency that is recalling a report knows whether it is being recalled for a FISA-compliance reason. It appears to the Court that a substantial improvement would be for the recalling agency, when applicable, to communicate to recipient agencies that a report is being recalled for a FISA-compliance reason and to request that they take steps to remove it from their systems and prevent its use or disclosure. The Court is directing the government to submit a written report by February 28, 2020, specifying, as applicable: (1) steps taken or to be taken by the FBI, NSA, CIA, and NCTC to identify to recipient agencies when reports are recalled for a FISA-compliance reason; (2) other steps the government has taken or will take to improve processes for identifying and removing reports that are recalled for FISA-compliance reasons; and (3) an anticipated timetable for completing any steps that remain to be taken.

**D. NSA Purge Backlog**

The October 18, 2018, Opinion discussed NSA’s backlog of purge-discovery orders, which had resulted in significant delays in placing information acquired pursuant to Section 702 on NSA’s Master Purge List. *See* October 18, 2018, Opinion at 128-30. NSA had eliminated this backlog by the time that Opinion was issued, but had not yet provided to the Court a proposed standard for determining whether a backlog emerges in the future. *Id.* at 130. On February 26, 2019, after reviewing the government’s proposal in that regard, the Court issued an

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

Order directing it to continue to take specified steps to ensure that information subject to purge is not included in a FISA application; report to the Court if there is a significant and persistent delay in NSA's purge process; and submit quarterly reports that assess the timeliness of NSA's purge process. See [REDACTED] Order, In re NSA's Purge Discovery Backlog for Information Acquired Pursuant to FISA, Feb. 26, 2019. The quarterly reports filed to date indicate that NSA's purge process has been operating in a timely manner. See Docket No. [REDACTED] [REDACTED] Government's First Quarterly Report in Response to the Court's Order of February 26, 2019, June 6, 2019; Docket No. [REDACTED] Government's Second Quarterly Report in Response to the Court's Order of February 26, 2019, Nov. 22, 2019.

**E. Other Incidents of Non-Compliance**

The government has identified a number of other incidents of noncompliance since the October 18, 2018, Opinion. For example, NSA sometimes has tasked selectors for acquisition without properly implementing the pre-tasking requirements of its targeting procedures. See, e.g., September 2019 Quarterly Report at 6-32. In other instances, an agency failed to timely detask selectors when required to do so under applicable targeting procedures, for reasons such as human error, communication failures among agencies, and misunderstanding of the procedures. See, e.g., id. at 33-73. There have also been cases in which the FBI did not properly establish a review-team process to protect attorney-client communications after a Section 702 target had been charged with a federal crime. See Supplemental Notice of Compliance Incident Regarding Implementation of the Review Team Requirements in the FBI's FISA Minimization Procedures, Sept. 30, 2019. Those errors stemmed from a misunderstanding of the requirements

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

of Section III.D.5.a of the FBI's minimization procedures or, in one instance, from a coding change in [REDACTED] d. In another example, a [REDACTED]

See September 2019 Quarterly Report at 124.

After considering the matters discussed above and other incidents reported by the government and assessing the overall state of implementation of the current targeting, querying, and minimization procedures, the Court finds that the proposed procedures, as reasonably expected to be implemented, comply with applicable statutory and Fourth Amendment requirements. It will, however, continue to monitor the government's implementation of the procedures, especially regarding U.S.-person queries.

## VII. CONCLUSION

For the foregoing reasons, the Court finds that:

(1) The 2019 Certifications, as well as the certifications in the Prior 702 Dockets, as thereby amended, contain all the required statutory elements;

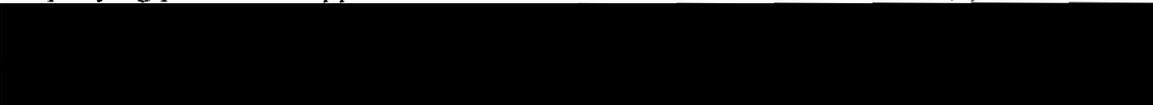
(2) The targeting procedures for acquisitions conducted pursuant to the 2019 Certifications are consistent with the requirements of Section 702(d) and of the Fourth Amendment;

(3) With respect to information acquired under the 2019 Certifications, the minimization procedures and querying procedures are consistent with the requirements of Section 702(e) and Section 702(f)(1), respectively, and of the Fourth Amendment;

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

(4) With respect to information acquired under the certifications in the Prior 702 Dockets, as amended, the minimization procedures (including, as referenced therein, the requirements of the respective agencies' querying procedures) are consistent with the requirements of Section 702(e) and of the Fourth Amendment; and

(5) The querying procedures approved for use in connection with DNI/AG 702(h) Certification 

 are consistent with the requirements of Section 702(f)(1) and of the Fourth Amendment.

(The Court does not make an equivalent finding regarding the other certifications in the Prior 702 Dockets because Section 702(f) only applies “with respect to certifications submitted under [Section 702(h)] . . . after January 1, 2018.” Reauthorization Act § 101(a)(2).); and, accordingly,

IT IS HEREBY ORDERED AS FOLLOWS:

- (1) The government's September 17, 2019, Submission is approved, as set out below:
- a. The 2019 Certifications and the certifications in the Prior 702 Dockets, as amended, are approved;
  - b. The use of the targeting procedures for acquisitions conducted pursuant to the 2019 Certifications is approved;
  - c. With respect to information acquired under the 2019 Certifications, the use of the minimization procedures and querying procedures is approved; and
  - d. With respect to information acquired under the certifications in the Prior 702 Dockets, the use of the minimization procedures (including, as referenced therein, the requirements of the respective agencies' querying procedures) is approved;

~~TOP SECRET//SI//ORCON//NOFORN~~

Page 79

~~TOP SECRET//SI//ORCON//NOFORN~~

(2) Separate orders memorializing the dispositions described above are being issued contemporaneously herewith pursuant to Section 702(j)(3)(A);

(3) The following provisions of the October 18, 2018, Opinion shall remain in effect for the reasons stated therein. Prospectively, the government need not comply with reporting requirements imposed by the October 18, 2018, Opinion, or other FISC opinions and orders in the Prior 702 Dockets, except as reiterated below:

a. Raw information obtained by NSA's upstream Internet collection under Section 702 shall not be provided to the FBI, the CIA or NCTC unless it is done pursuant to revised minimization procedures that are adopted by the AG and DNI and submitted to the FISC for review in conformance with Section 702;

b. On or before December 31 of each calendar year, the government shall submit a written report to the FISC: (a) describing all administrative-, civil- or criminal-litigation matters necessitating preservation by the FBI, NSA, CIA or NCTC of Section 702-acquired information that would otherwise be subject to destruction, including the docket number and court or agency in which such litigation matter is pending; (b) describing the Section 702-acquired information preserved for each such litigation matter; and (c) describing the status of each such litigation matter;

c. The government shall promptly submit a written report describing each instance in which an agency invokes the provision of its minimization or querying procedures providing an exemption for responding to congressional mandates, as discussed in Part IV.D.3 of the October 18, 2018, Opinion. Each such report shall describe the circumstances of the

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

deviation from the procedures and identify the specific mandate on which the deviation was based;

d. The government shall promptly submit in writing a report concerning each instance in which FBI personnel accessed unminimized Section 702-acquired contents information that was returned by a query that used a U.S.-person query term and was not designed to find and extract foreign-intelligence information. The report should include a detailed description of the information at issue and the manner in which it has been or will be used for analytical, investigative, or evidentiary purposes. It shall also identify the query terms used to elicit the information and provide the FBI's basis for concluding that the query was consistent with applicable procedures. The government need not file such a report for a query for which it files an application with the FISC pursuant to Section 702(f)(2);

e. The government shall continue to submit reports to the Court on a quarterly basis on its use [redacted] under Section 702. This report shall: (i) describe

[redacted]

(ii) explain how the government is ensuring that it will only acquire

communications to or from a Section 702 target [redacted] and (iii)

describe methods the government is using to monitor compliance with the abouts limitation [redacted]

[redacted]

and report on the results of such monitoring;

f. No later than ten days after tasking for upstream collection under Section 702 a

[redacted]

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

[REDACTED] the government shall submit a notice to the Court. This notice shall: (i) describe [REDACTED] (ii) explain how [REDACTED] will comply with the above limitation; and (iii) describe steps that will be taken during the course of the proposed acquisition to ensure that [REDACTED] is only acquiring communications to or from authorized Section 702 targets; and

g. The reporting requirement regarding retention of unminimized Section 702 information in FBI archival systems that appears at page 138 of the October 18, 2018, Opinion shall remain in effect for instances of retention that the government is currently obligated to report pursuant to that requirement; and

(4) For the reasons stated herein, the government shall comply with the following requirements:

a. The government shall submit a report by February 28, 2020, specifying, as applicable: (1) steps taken or to be taken by the FBI, NSA, CIA, and NCTC to identify to recipient agencies when reports are recalled for FISA-compliance reasons; (2) other steps the government has taken or will take to improve processes for identifying and removing reports that are recalled for FISA-compliance reasons; and (3) an anticipated timetable for completing any steps that remain to be taken; and

b. On or before March 26, 2021, the government shall submit an update to each agency's UAM submission filed on March 29, 2019. As with the latter, the update shall describe the UAM activities being undertaken by each agency and provide an assessment as to whether

~~TOP SECRET//SI//ORCON//NOFORN~~

~~TOP SECRET//SI//ORCON//NOFORN~~

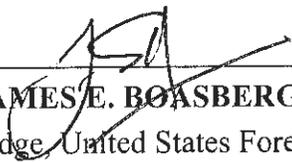
those activities are being conducted in a manner consistent with applicable Section 702

procedures. In particular, the submission shall describe:

- (1) the nature and scope of UAM activities being conducted, the user activities subjected to monitoring, and the types of information being captured;
- (2) the repositories in which UAM data resides, and the access restrictions and controls in place to limit access to such repositories;
- (3) the authorized purposes for which such data may be accessed; and
- (4) the number and types of personnel who have access to UAM data, and the training required for such personnel to obtain such access.

The submission shall also provide an updated assessment of the amount of unminimized Section 702-acquired information stored in the UAM repositories of each agency, based on the nature and scope of the activities being conducted, the agency's experience with finding such information in its UAM repositories, and any other relevant consideration.

ENTERED at 3:30 p.m. Eastern Time this 6<sup>th</sup> day of December, 2019.

  
 \_\_\_\_\_  
**JAMES E. BOASBERG**  
 Judge, United States Foreign  
 Intelligence Surveillance Court

~~TOP SECRET//SI//ORCON//NOFORN~~

I, [redacted] Deputy Clerk, FISC, certify that this document is a true and correct copy of the original [redacted]