THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

HTTP://WWW.BLACKVAULT.COM

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

All redacted information exempt under b(1) and/or b(3) except where otherwise noted.

EXHIBIT A

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

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
[redacted] PM 1:43
CLERK OF COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

Docket Number: PR/TT

EXHIBIT A

**DECLARATION OF GENERAL KEITH B. ALEXANDER,
UNITED STATES ARMY,
DIRECTOR OF THE NATIONAL SECURITY AGENCY**

(U) I, General Keith B. Alexander, declare as follows:

1. (U) I am the Director of the National Security Agency ("NSA"), an intelligence agency within the United States Department of Defense, and have served in this position since 2005. I currently hold the rank of General in the United States Army and, concurrent with my current assignment as Director of the NSA, I also serve as the

Classified by: NSA/CSSM 1-52, Dated 8 January, 2007
Reason: 1.4(c)
~~Declassify on:~~ [redacted]

Chief of the Central Security Service and as the Commander of the United States Cyber Command. Prior to my current assignment, I have held other senior supervisory positions as an officer of the United States military, to include service as the Deputy Chief of Staff, Headquarters, Department of the Army; Commander of the United States Army's Intelligence and Security Command; and the Director of Intelligence, United States Central Command.

2. (U) As the Director of the NSA, I am responsible for directing and overseeing all aspects of NSA's cryptologic mission, which consists of three functions: to engage in signals intelligence ("SIGINT") activities for the United States Government, to include support to the Government's computer network attack activities; to conduct activities concerning the security of United States national security telecommunications and information systems; and to conduct operations security training for the United States Government. Some of the information NSA acquires as part of its SIGINT mission is collected pursuant to Orders issued under the Foreign Intelligence Surveillance Act of 1978, as amended. My statements herein are based on (i) my personal knowledge of SIGINT collection and NSA operations, (ii) my review of the Application, (iii) information available to me in my capacity as the Director of the NSA, about NSA's previous and continuing SIGINT collection activities pursuant to FISA, and (iv) the advice of counsel.

(U) PURPOSE OF DECLARATION

3. ~~(S//SI)~~ I make this Declaration in support of the Government's Application seeking authority to install and use pen registers and trap and trace devices, at [redacted] facilities described in Tab 1 to this Declaration ("Facilities"), in order to obtain information about [redacted] "Foreign Powers") pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA"). As set forth in greater detail below, the requested authority will enable NSA to continue its efforts to discover the Foreign Powers and unknown persons in the United States and abroad affiliated with one or more of the Foreign Powers, and their communications, and to disseminate such information to support the efforts of the United States, and in particular of the Federal Bureau of Investigation (FBI), to detect and prevent terrorist acts against United States interests. This will be accomplished by collecting[1] certain "metadata"[2]—not the "contents" as defined by 18 U.S.C. § 2510(8) of the

---

[1] ~~(TS//SI//NF)~~ For purposes of this Declaration, "collect," "collecting," and "collection" include any and all elements of the recording, decoding, and/or capturing of a category or type of metadata (defined below) associated with an Internet communication (defined below), and all inferences drawn from metadata associated with an Internet communication, prior to ingestion into an NSA repository.

[2] ~~(TS//SI//NF)~~ The term "metadata," as used in this Declaration, includes all dialing, routing, addressing, or signaling information associated with an Internet communication (defined below) not concerning the substance, purport, or meaning of the communication and all other information associated with an Internet communication not concerning the substance, purport, or meaning of the communication. The categories or types of metadata that the Government will collect pursuant to the authority requested in the Government's Application are described in the attached Tab 2.

communications [redacted] — and then querying that metadata with "seed" identifiers[4] that are suspected to have terrorist affiliations.

~~(TS//SI//NF)~~ WORLDWIDE PRESENCE OF THE FOREIGN POWERS

4. (S//SI) [redacted] Indeed, as stated in the Declaration of Michael E. Leiter, Director of the National Counterterrorism Center (NCTC) ("NCTC Declaration"), which has been filed with the Court at docket number [redacted] NCTC Decl. at 7. As noted in the NCTC Declaration, [redacted]

[redacted]

[3] ~~(TS//SI//NF)~~ The term "Internet communications," as used in this Declaration, includes communications via electronic mail (e-mail) [redacted]

[4] [redacted]

[redacted]

[redacted] NCTC Decl. at 7.

5. ~~(S//SI)~~ [redacted]

[redacted]

6. ~~(TS//SI)~~ [redacted]

[redacted]

[redacted]

5 [redacted]

[redacted]

7. ~~(TS//SI)~~ [redacted]

[redacted]

[redacted]

8. ~~(TS//SI//NF)~~ Accordingly, the information set forth above, along with NSA's traditional SIGINT collection under Executive Order 12333, as amended, and Court-authorized electronic surveillance demonstrate that the Foreign Powers operate in and communicate to and from locations worldwide.

~~(S//SI)~~ USE OF INTERNET COMMUNICATIONS BY TERRORIST ORGANIZATIONS

9. ~~(TS//SI//NF)~~ [redacted]

[redacted]

10. ~~(TS//SI//NF)~~ [redacted]

[redacted]

[redacted]

11. ~~(TS//SI//NF)~~ [redacted]

[redacted]

[redacted]

12. ~~(TS//SI//NF)~~ [redacted]

[redacted]

13. ~~(TS//SI//NF)~~ Previous surveillance authorities granted by the Court, initially in July 2004 and most recently in [redacted], enabled NSA to support the efforts of the United States Government to detect and prevent terrorist acts against United States interests by collecting specific categories of metadata from e-mail [redacted] communications, and then conducting analysis of a subset of this metadata associated with e-mail [redacted] associated with the Foreign Powers.[6] As described in Tab 2, NSA is seeking to again collect metadata associated with e-mail[7] [redacted] communications.

---

[6] ~~(TS//SI//NF)~~ On [redacted] when the Order in docket number PR/TT [redacted] lapsed, the Court entered a Supplemental Order in docket number PR/TT [redacted] and previous dockets, directing that the Government "shall not access the information obtained pursuant to the FISC's orders in this matter for any analytic or investigative purpose," unless the access is necessary to protect against an imminent threat to human life. Supplemental Order, Docket Number PR/TT [redacted], at 4-5.

~~(TS//SI//NF)~~ The ability of NSA to access the information collected under docket number PR/TT [redacted] and previous dockets is vital to NSA's ability to carry out its counterterrorism intelligence mission. If NSA is not able to combine information it collects prospectively with the information it collected under docket number PR/TT [redacted] and previous dockets, there will be a substantial gap in the information available to NSA. This gap would result in a degradation of NSA's ability to glean counterterrorism-related intelligence from information collected under docket number PR/TT [redacted] and previous dockets. Accordingly, the Government is seeking authority to access the information collected under docket number PR/TT [redacted] and previous dockets and treat it in accordance with these procedures.

[7] ~~(TS//SI//NF)~~ For purposes of this Declaration, "e-mail communications" includes (1) all e-mail messages sent between e-mail users, [redacted]

14. ~~(S//SI)~~ Intelligence Community investigation and analysis has shown that individuals associated with the Foreign Powers have come to rely heavily on Internet communications as a way to convey closely held activities, to include operational planning. Intelligence Community analysis and reporting further demonstrates that: (a) [redacted] Intelligence Community analysis and reporting also demonstrates that terrorist organizations associated with [redacted] as more fully described in paragraphs 6-7 above, [redacted]

15. ~~(TS//SI//NF)~~ Use by terrorists of the specific techniques noted above demonstrates why it is necessary for NSA to collect bulk metadata associated with Internet communications at the Facilities to be able to identify and track the communications of the Foreign Powers.

~~(S//SI)~~ METADATA NSA SEEKS TO ACCESS AND NSA'S COLLECTION AND PROCESSING OF THE METADATA

16. ~~(TS//SI//NF)~~ The accompanying Application requests authority to install and use pen registers and trap and trace devices at the Facilities. Each such Facility is a [redacted]. Internet communications of the Foreign Powers are among those Internet communications carried on those facilities. The categories or types of metadata that the Government will collect pursuant to the authority requested in the Application are described in Tab 2 to this Declaration.

17. ~~(TS//SI//NF)~~ [redacted]

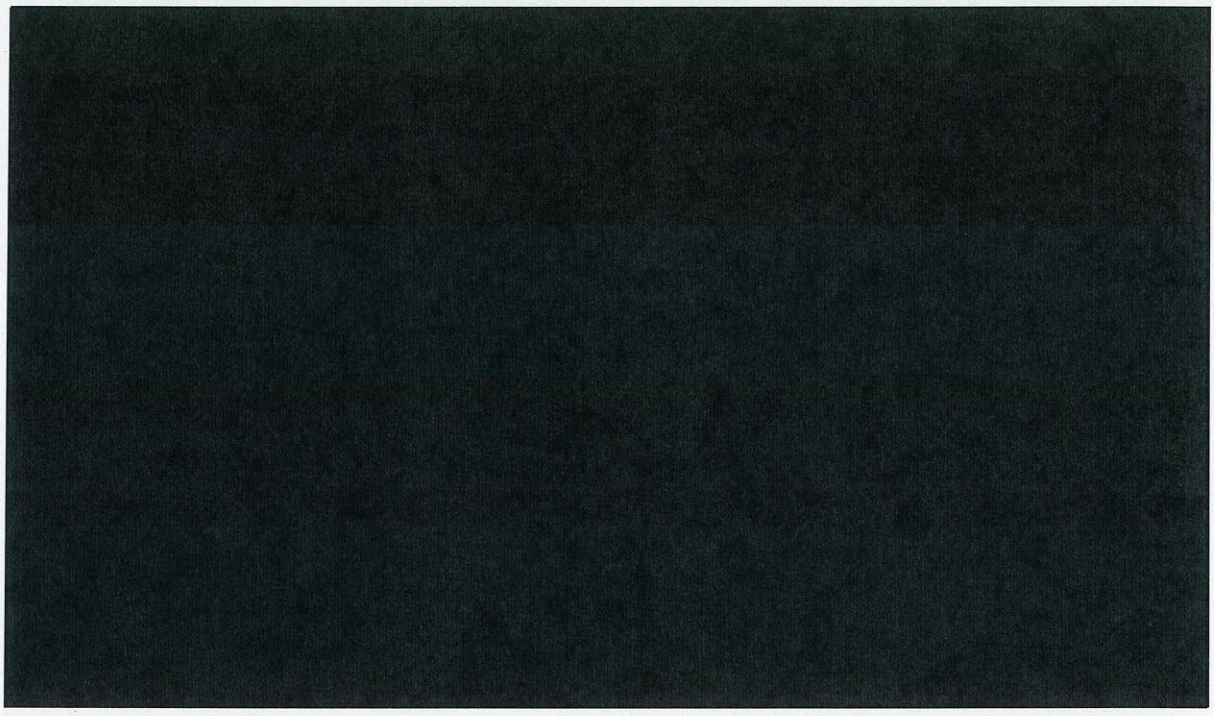
[redacted]

18. ~~(TS//SI//NF)~~ [redacted]

[redacted]

- [redacted]

For example, a device may identify that a particular communication was generated by a [redacted] user, [redacted] With this knowledge, the device will further analyze the [redacted] communication to determine [redacted]



19. (~~TS//SI//NF~~) NSA's collection and processing systems perform multi-level validation on much of the information being collected prior to storing it in NSA's

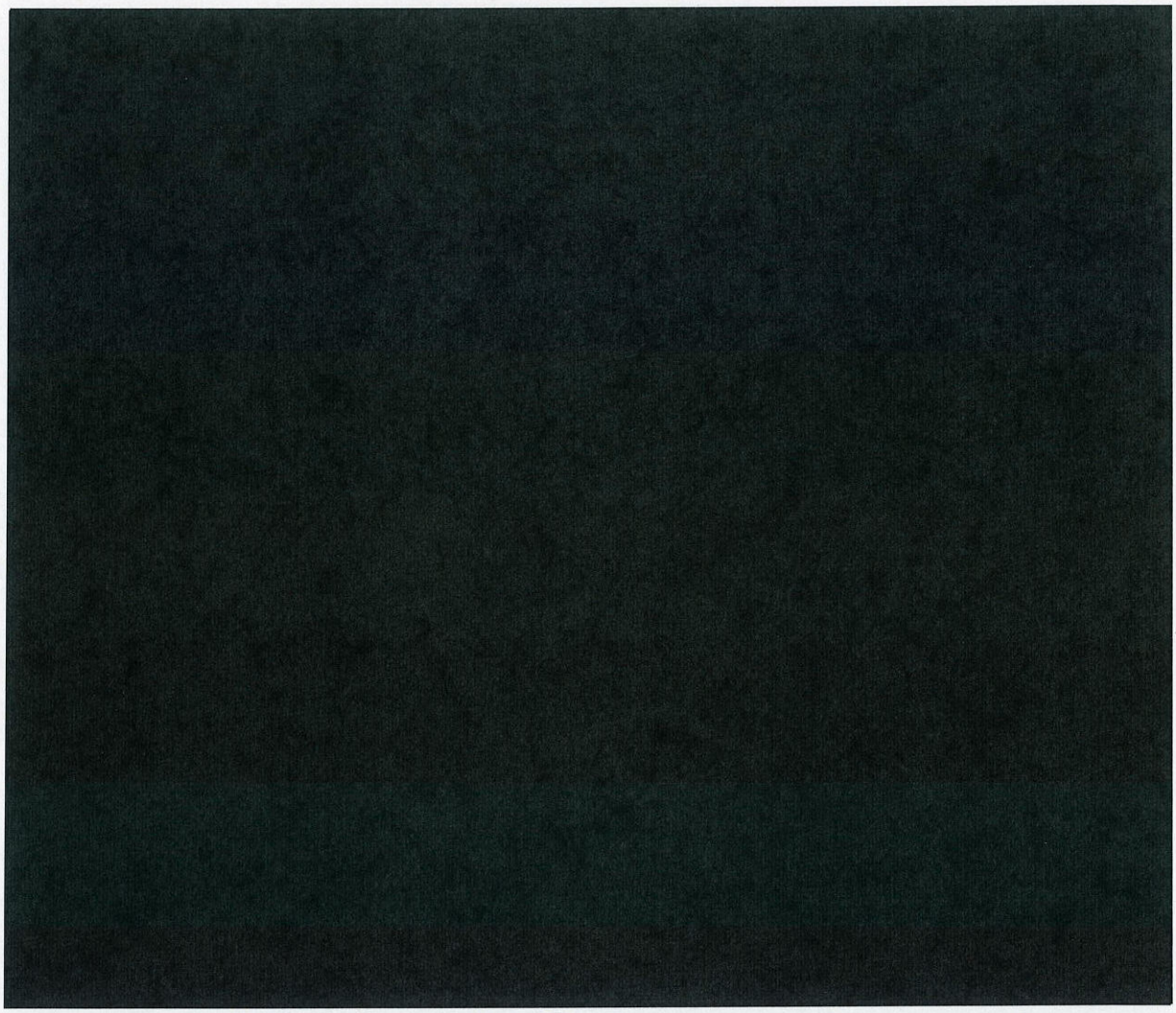
repositories. [redacted]

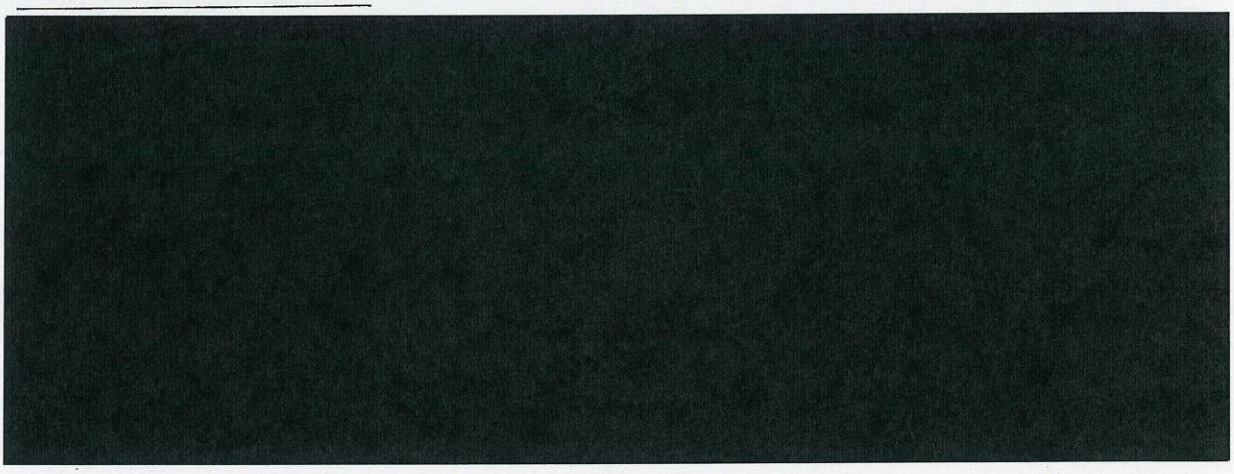
[redacted]

20. ~~(TS//SI//NF)~~ [redacted]

[redacted]

[redacted]





~~(S//SI)~~ WHY NSA SEEKS TO COLLECT THIS METADATA AND HOW NSA ANALYZES THE METADATA

21. ~~(TS//SI//NF)~~ To better ensure success in its counterterrorism intelligence mission, NSA needs to have access to the accumulated pool of metadata described in the Application and this Declaration. It is not possible to target collection solely to known terrorist Internet communications accounts and at the same time use the advantages of metadata analysis to discover the enemy. This is because the Foreign Powers take affirmative and intentional steps to disguise and obscure their Internet communications and their identities. They do this using a variety of tactics, [redacted] [redacted] The most effective means by which NSA analysts are able to continuously keep track of the Foreign Powers making use of such tactics is to obtain and maintain access to metadata repositories that will permit these tactics to be uncovered.

22. ~~(S//SI)~~ Because it is impossible to determine in advance what metadata will turn out to be valuable in tracking, identifying, characterizing and exploiting a terrorist, collecting metadata in the manner set out above is vital for success. Likewise,

it is impossible to have a complete prospective awareness of all terrorist threats at any given time. For these reasons, obtaining the fullest intelligence benefit from terrorist-related Internet communications requires that metadata be collected in bulk and also be kept available for retrospective, or historical, analysis for a reasonable period of time. Analysts know that the terrorists' Internet communications are located somewhere in the billions of data bits traversing the Facilities; what they cannot know ahead of time is exactly where. If metadata is not collected by the Government at the time that Internet communications are transmitted, that data disappears and is lost forever.

23. (~~TS//SI//NF~~) The ability to accumulate the metadata in repositories and set it aside for carefully controlled searches and analysis will substantially increase NSA's ability to detect and identify the Foreign Powers and those individuals affiliated with them. The NSA will conduct contact chaining queries of the metadata repositories to determine the contacts and/or connections of particular terrorist-associated identifiers.

24. (~~TS//SI//NF~~) Contact chaining queries of the metadata will begin with a RAS-approved seed, and will return only that metadata within two "hops" of the seed.[12]

---

[12] (~~TS//SI//NF~~) The first "hop" from a seed returns results including all identifiers (and their associated metadata) with a contact and/or connection with the seed. The second "hop" returns results that include all identifiers (and their associated metadata) with a contact and/or connection with an identifier revealed by the first "hop." Going out to the second "hop" enhances NSA's ability to find, detect and identify the Foreign Powers and those affiliated with them by greatly increasing the chances that previously

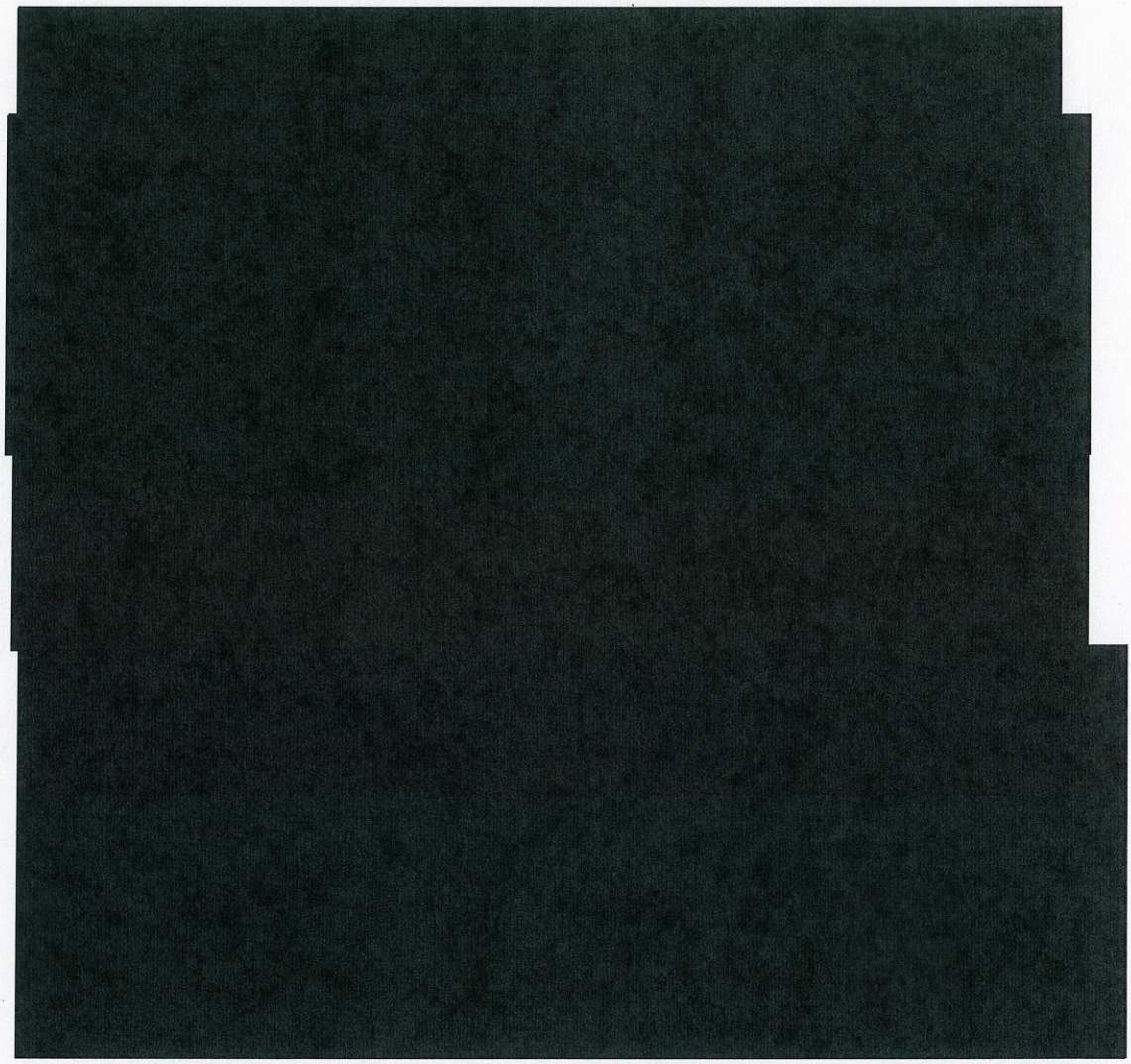
Metadata associated with a seed and these contacts or connections will be integrated with metadata acquired under other authorities for further analysis. As appropriate, the results of such queries will be shared within NSA for further SIGINT analysis, and ultimately disseminated to support the efforts of the United States, and in particular of the FBI, to detect and prevent terrorist acts against United States interests.

25. (~~TS//SI//NF~~) Once NSA conducts a query of a RAS-approved seed, NSA is then able to apply other analytic methods and techniques to the query results. Metadata analysis of query results is an essential aspect of SIGINT analysis that allows NSA to exploit the communications of a mobile, global target set that commonly uses free, widely available Internet communications. Successful exploitation of the Internet communications of the Foreign Powers requires that NSA is in constant state of development and discovery, [redacted] Metadata analysis contributes to this critical target monitoring, development and discovery by providing information that an analyst can use to determine various intelligence information, including but not limited to [redacted]

unknown Foreign Power-associated identifiers may be uncovered. A "seed" e-mail address, for example, may be in contact with a previously unknown e-mail address. Chaining out to the second hop to examine the contacts made by that e-mail address may reveal a contact with other e-mail address already known to be associated with a Foreign Power, thus establishing that the previously-unknown e-mail address is itself likely associated with a Foreign Power.

[redacted]

[redacted] These kinds of analysis are equally applicable in the ongoing development of known targets as well as in the discovery of new targets. In particular, the use of a RAS-approved seed to query NSA's repository of historical Internet communications metadata can help the Government discover previously unknown contacts between the seed identifier and [redacted]



26. ~~(TS//SI//NF)~~ The ability to collect metadata in bulk is also necessary for the purpose of retrospective (historical) analysis. Retrospective analysis not only allows for NSA analysts to pursue newly found leads, it also facilitates NSA's ability to maintain more complete coverage of a known target and triage major events. To the extent that historical connections are important to understanding a newly-identified target,

collected metadata may contain unique links, pointing to potential targets and/or identifiers that otherwise would be missed. Historical metadata analysis (using multiple sources available to NSA analysts) is a necessary and lucrative resource for discovering and understanding the communications [redacted] of a terrorist suspect before a potential threat materializes into an actual threat.[13] Additionally, the intelligence gleaned from the metadata may be used to inform further analysis, [redacted] providing the substance of NSA end-product intelligence reporting to the FBI and other members of the United States Intelligence Community, and providing new leads for tasking/targeting. Furthermore, metadata analysis helps to refine and steer [redacted]

27. (~~S//SI~~) Were NSA to use pen registers and trap and trace devices targeted individually at specific terrorist-associated [redacted] to collect metadata associated with the identifiers in contact with [redacted] the Internet communications identifiers in contact with the first-tier of identifiers, *i.e.*, going "two

[redacted]

hops out"—that process would potentially entail the submission of thousands of pen register and trap and trace device applications per year. As explained above, acquiring metadata using individually-targeted pen registers and trap and trace devices would not permit NSA to accumulate a metadata repository that could broadly discover relevant historical information about newly-found identifiers associated with suspected terrorists. Using such an individually-targeted approach would deprive NSA of the vastly more powerful analytic potential offered by a historic repository of metadata. For example, if investigators find a new identifier [redacted] by revealing the contacts that were made by the-now-disused account in the past—contacts that may in turn reveal other terrorist accounts that continue to be active.

(~~TS//SI//NF~~) DESCRIPTION OF NSA's COLLECTION, STORAGE, ANALYSIS, DISSEMINATION AND RETENTION OF THE METADATA

28. (~~TS//SI//NF~~) Collection of the metadata. The specified person that controls each Facility [redacted]

[redacted]

[redacted][14]

[redacted]

29. (~~TS//SI//NF~~) Administration of the Metadata Repositories. NSA will store and process the collected metadata in repositories within secure networks under NSA's control.[15] The metadata will carry unique markings such that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to the

[redacted]

[15] (~~TS//SI//NF~~) NSA will also maintain the metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA will ensure that any access or use of the metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

authority. Trained and authorized technical personnel[16] may access the metadata to perform those processes needed to make the metadata usable for intelligence analysis. For example, these processes may include metadata validation; the defeat of the collection, processing or analysis of metadata[17] associated with [redacted] other metadata deemed of little use for metadata analysis purposes; the maintenance of records to demonstrate compliance with the terms of the authority; and the development and testing of technologies to be used with the metadata.

30. ~~(TS//SI//NF)~~ [redacted] Other Unwanted Metadata. Technical personnel may query the metadata using identifiers that have not been RAS-approved for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes. An authorized technician may query the metadata with a non-RAS-approved identifier to determine whether that identifier [redacted] If so, the technician could share the results of that query, *i.e.*, the identifier and the fact that [redacted] with authorized personnel (including those responsible for the identification and defeat of [redacted]

---

16 ~~(TS//SI//NF)~~ Certain technical personnel, specifically the personnel responsible for [redacted] will not receive special training regarding the procedures and restrictions for the collection, storage, analysis, dissemination and retention of the metadata.

17 ~~(TS//SI//NF)~~ Defeat may occur during analysis. For example, an analyst might be made aware of a [redacted] either through query results or through access to target knowledge databases or other sources, and may then choose to block or disregard information related to that identifier.

[redacted] other unwanted metadata from any of NSA's various metadata repositories), but could not share any other information from the results of that query for intelligence analysis purposes.

31. (~~TS//SI//NF~~) Procedures for Conducting Queries and Other Analysis.

(a) NSA analysts[18] may conduct contact chaining queries of the metadata for the purpose of obtaining foreign intelligence information using identifiers approved as "seeds" pursuant to the RAS approval process described below. NSA will ensure, through adequate and appropriate technical and management controls, that no queries of the metadata will be conducted for intelligence analysis purposes using an identifier that has not been RAS-approved.

(i) (~~TS//SI//NF~~) Identifiers to be used as "seeds" with which to query the metadata may be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval will be given only after the designated approving official has

[18] (~~TS//SI//NF~~) Under previous Court Orders, NSA safeguarded against queries using non-RAS-approved seeds by limiting the number of analysts with authority to query the metadata and providing those analysts special training to emphasize the importance of the proper use of RAS-approved seeds. NSA monitored the effectiveness of these safeguards, by logging all analytic queries for auditing purposes. In [redacted] NSA implemented technical controls, which block any analytic query of the metadata with a non-RAS-approved seed. In the accompanying Application, NSA is also seeking authority to share query results, as needed, throughout NSA's analytic enterprise. Because of the new technical controls that protect against improper queries, and because NSA is seeking authority for broader sharing of query results among NSA analysts, the limitation on the number of analysts with query authority would no longer serve a meaningful compliance purpose. Accordingly, NSA has not proposed to limit the number of analysts with query authority under this Application. The logging of analytic queries, as described in paragraph 31(b), will continue to serve as a compliance measure.

determined that, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that the identifier is associated with a Foreign Power; provided, however, that NSA's Office of General Counsel (OGC) shall first determine that any identifier reasonably believed to be used by a United States person is not regarded as associated with a Foreign Power solely on the basis of activities that are protected by the First Amendment to the Constitution.

(ii) (~~TS//SI//NF~~) Identifiers that are the subject of electronic surveillance and/or physical search authority of the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by agents of a Foreign Power, including any reasonably believed to be used by United States persons, may be deemed RAS-approved for the period of FISC-authorized electronic surveillance and/physical search without further review and approval by an NSA designated approving official. The preceding sentence shall not apply to identifiers under surveillance pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) (~~TS//SI//NF~~) A determination by a designated approving official that an identifier is associated with a Foreign Power shall be effective for 180 days for any identifier reasonably believed to be used by a United States person; and one year for all other identifiers.

(b) (~~TS//SI//NF~~) Whenever the metadata is queried for intelligence analysis purposes or using intelligence analysis query tools, an auditable record of the activity will be generated.

32. (~~TS//SI//NF~~) Sharing, Minimization, and Dissemination Procedures. Results derived from any RAS-approved query of the metadata may be shared, prior to

minimization, for intelligence analysis purposes among NSA analysts.[19] NSA will apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) to any results from queries of the metadata disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of NSA, the Deputy Director of NSA, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operation Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.[20] Notwithstanding the above requirements, NSA may share results derived from intelligence analysis queries of the metadata, including U.S. person identifying information, with Executive Branch personnel (1) in order to enable them to determine whether the information contains

---

[19] (~~TS//SI//NF~~) In addition, NSA may apply the full range of SIGINT analytic tradecraft to the metadata associated with RAS-approved seeds and the metadata associated with contacts or connections within two "hops" of those seeds.

[20] (~~S~~) In the extraordinary event that NSA determines that there is a need to disseminate information identifying a U.S. person that is related to foreign intelligence information, as defined by 50 U.S.C. § 1801(e), other than counterterrorism information and that is necessary to understand the foreign intelligence information or assess its importance, NSA will seek prior approval from the Court.

exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

33. (~~TS//SI//NF~~) Retention of the Metadata. Metadata collected by the pen registers and trap and trace devices shall be destroyed no later than five years (60 months) after its initial collection.

34. (~~TS//SI//NF~~) Oversight and Compliance. NSA and the National Security Division of the Department of Justice (NSD/DoJ) will conduct oversight of NSA's activities under this authority as outlined below. In addition, the Office of the Director of National Intelligence (ODNI) has independent responsibility over the Intelligence Community and must ensure that NSA's intelligence activities are conducted in compliance with the law. Accordingly, ODNI personnel may participate in the oversight activities described below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) will ensure that personnel with access to the metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the metadata and the results of queries of the metadata and will maintain records of such training. OGC will provide NSD/DoJ with copies of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC will monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC will consult with NSD/DoJ on all significant legal

opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD will be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives will meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of the metadata collected to ensure that only those categories or types of information described in Tab 2 are being collected. The results of this meeting will be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ will meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ will review a sample of the justifications for RAS approvals for identifiers used to query the metadata.

(vii) Prior to implementation, all proposed automated query processes will be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

--- Remainder of page intentionally left blank ---

35. (~~TS//SI//NF~~) Reporting. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of the queries made since the last report and NSA's application of the RAS standard. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report detailed information regarding any new facility proposed to be added to such authority and a description of any changes proposed in the collection methods, [redacted] [redacted] of the pen registers and trap and trace devices.

(U) I declare under penalty of perjury that the foregoing is true and correct.

Signed thi[redacted]

KEITH B. ALEXANDER
General, United States Army
Director, National Security Agency

TAB 1

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
[redacted] PM 1:43
CLERK OF COURT

[redacted]

Docket Number: PR/TT

TAB 1 TO THE DECLARATION OF GENERAL KEITH B. ALEXANDER, UNITED STATES ARMY, DIRECTOR OF THE NATIONAL SECURITY AGENCY

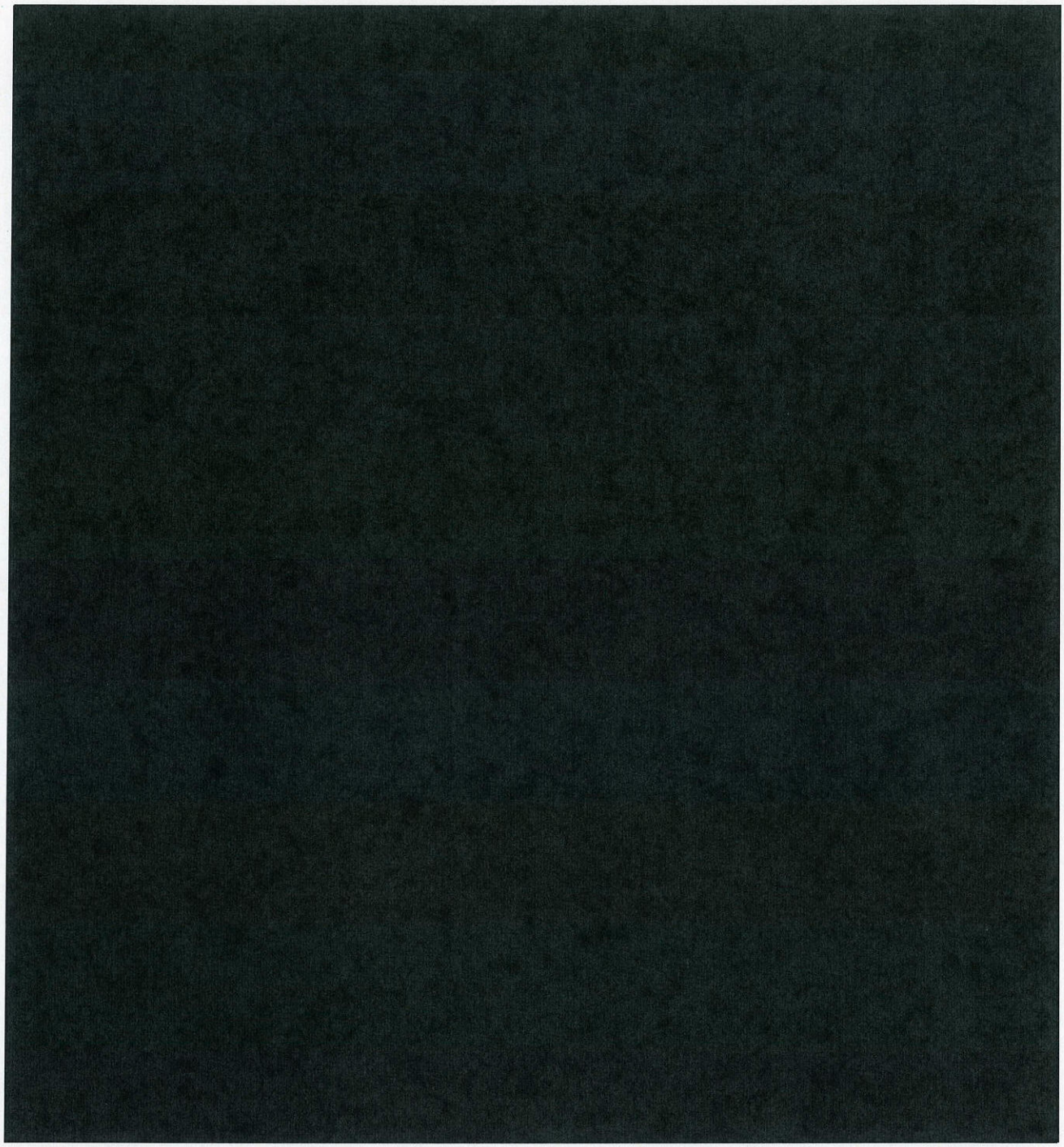
~~(TS//SI//NF)~~ As discussed in the Application and the Declaration that this Tab accompanies, the Government seeks authority to install and use pen registers and trap and trace devices, pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C., §§ 1801-1812, 1841-1846, as amended, on the Facilities described below.

Classified by: NSA/CSSM 1-52, Dated 8 January, 2007
Reason: 1.4(c)
~~Declassify on: 1 June 2035~~

~~(TS//SI//NF)~~ [redacted]

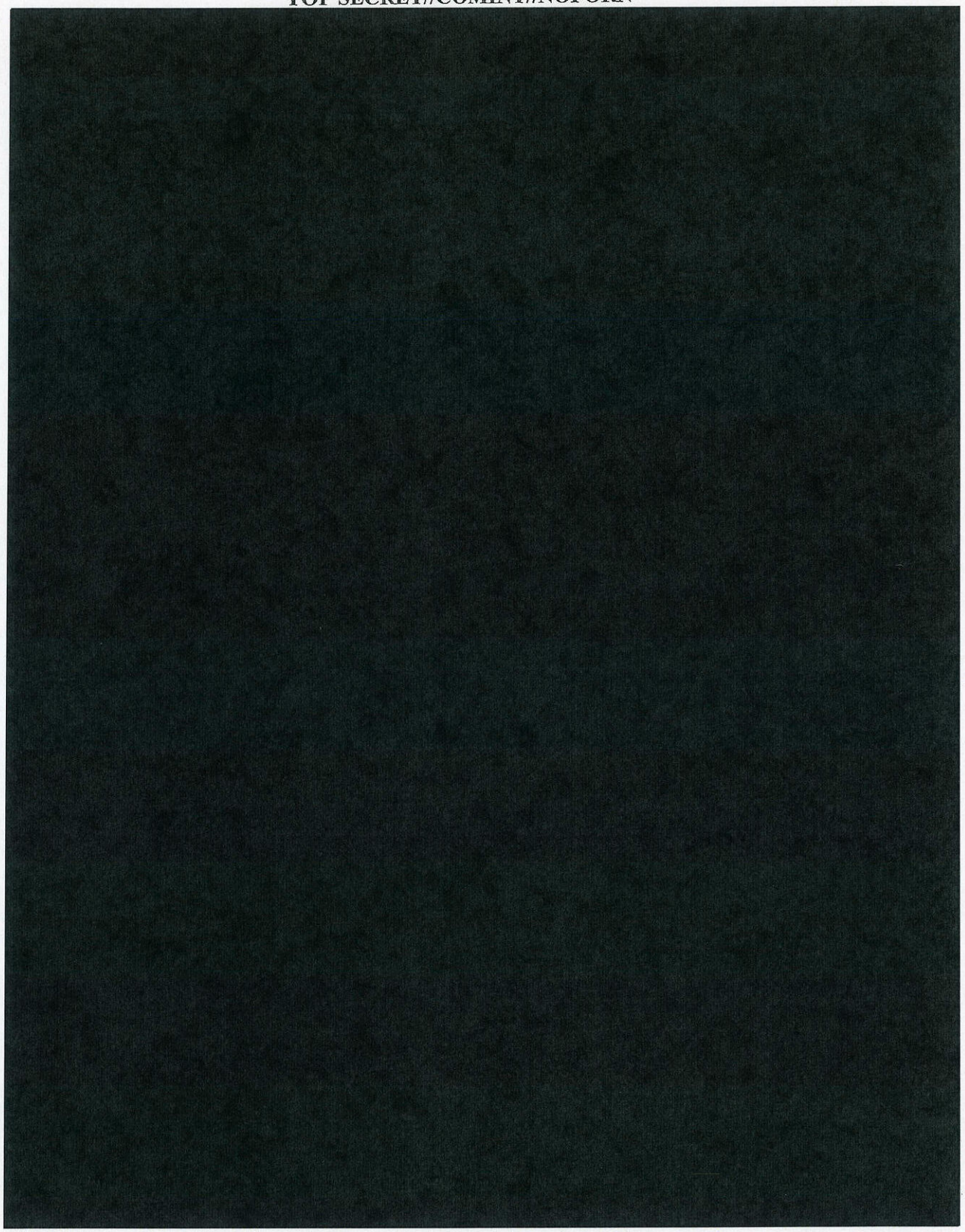
[redacted]

[redacted]



[redacted]

[1] (~~TS//SI//NF~~) [redacted]



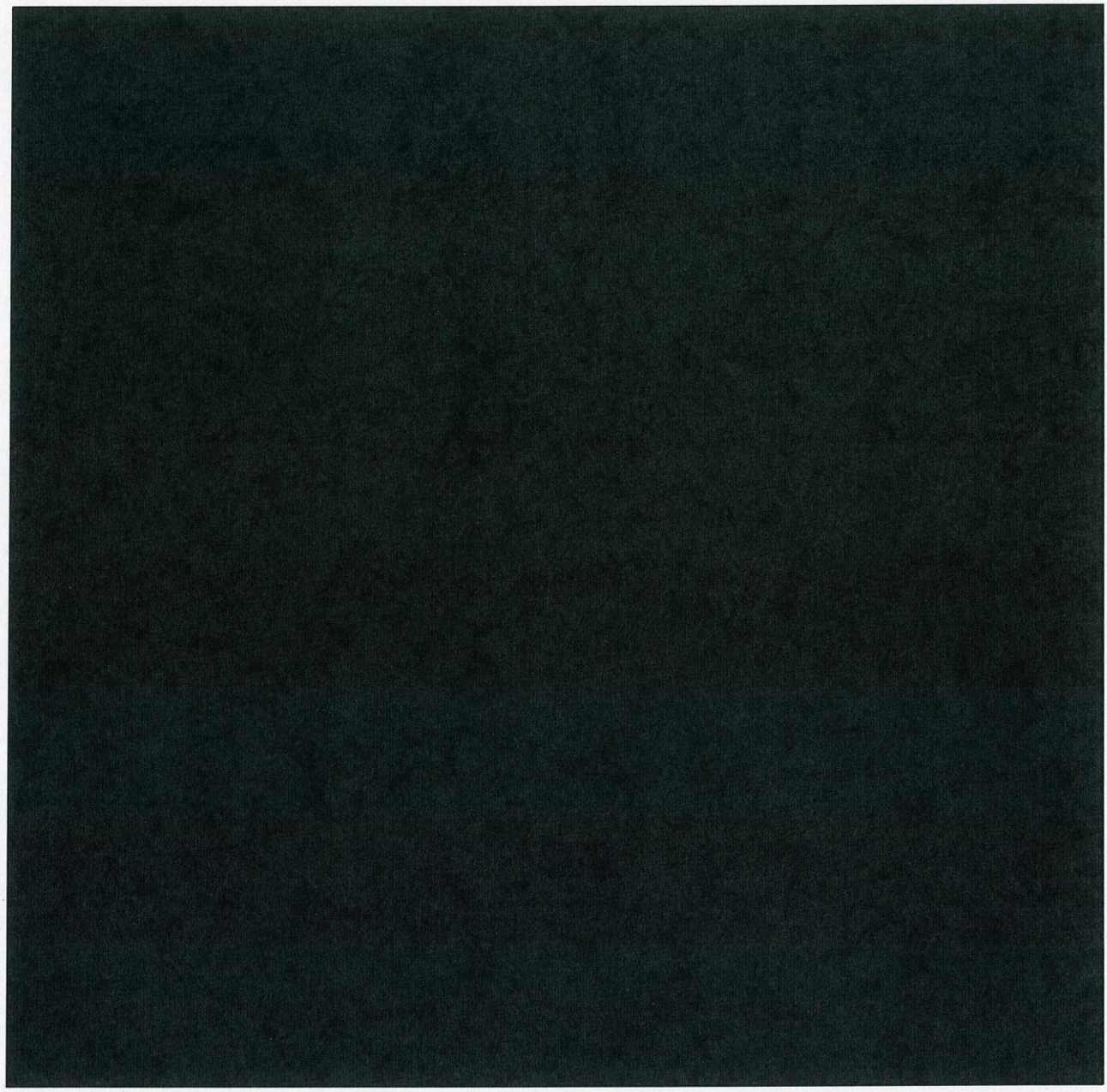
(~~TS//SI//NF~~ [redacted]

[redacted]

[redacted]







[redacted]

2 (~~TS//SI//NF~~) [redacted]

TAB 2

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
[redacted]
PM 1:43
CLERK OF COURT

[redacted]

Docket Number: PR/TT

TAB 2 TO THE DECLARATION OF GENERAL KEITH B. ALEXANDER, UNITED STATES ARMY, DIRECTOR OF THE NATIONAL SECURITY AGENCY

~~(TS//SI//NF)~~ Set forth below are descriptions of the categories and types of metadata[1] the Government will attempt to collect,[2] pursuant to the authority sought in

[1] ~~(TS//SI//NF)~~ For the purposes of this Tab, the term "metadata" includes all dialing, routing, addressing, or signaling information associated with an Internet communication (defined below) not concerning the substance, purport, or meaning of the communication and all other information associated with an Internet communication not concerning the substance, purport, or meaning of the communication.

[2] ~~(TS//SI//NF)~~ For the purposes of this Tab, "collect," "collecting," and "collection" include any and all elements of the recording, decoding, and/or capturing of a category or type of metadata associated with

Classified by: NSA/CSSM 1-52, Dated 8 January, 2007
Reason: 1.4(c)
~~Declassify on: 1 June 2035~~

the accompanying Application, from the Internet communications[3] accessed via the Facilities described in Tab 1. [redacted]

an Internet communication (defined below), and all inferences drawn from metadata associated with an Internet communication, prior to ingestion into an NSA repository.

[3] (~~TS//SI//NF~~) For the purposes of this Tab, the term "Internet communications" includes communications via electronic mail (e-mail) [redacted]

[4] (~~TS//SI//NF~~) For purposes of this Tab, "e-mail communications" includes (1) all e-mail messages sent between e-mail users [redacted]

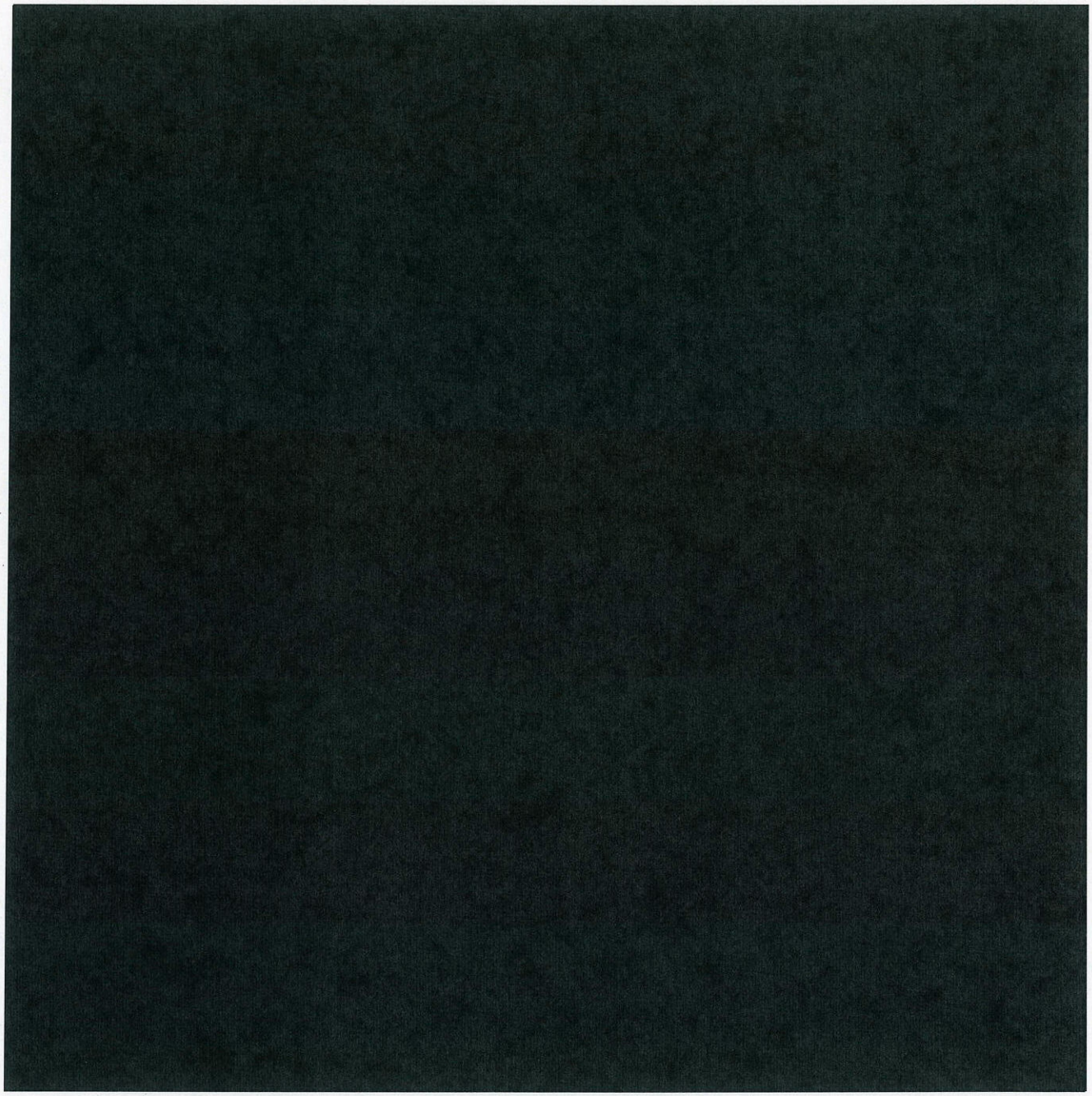
[5] (~~TS//SI//NF~~) For purposes of this Tab, [redacted]

[redacted]

[redacted]

[redacted]

6 (~~TS//SI//NF~~) [redacted]



[redacted]

[7] (~~TS//SI//NF~~) [redacted]

[8] (~~TS//SI//NF~~) [redacted]

[9] (~~TS//SI//NF~~) [redacted]

