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

~~TOP SECRET//COMINT//NOFORN//X1~~

FILED
KAREN E. SUTTON, CLERK
[redacted]
U.S. Foreign Intelligence Surveillance Court

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

Docket Number: PR/TT [redacted]

DECLARATION OF LIEUTENANT GENERAL MICHAEL V. HAYDEN,
UNITED STATES AIR FORCE,
DIRECTOR OF THE NATIONAL SECURITY AGENCY

(U) I, Lieutenant General Michael V. Hayden, United States Air Force, declare as follows:

1. (U) I am the Director of the National Security Agency (NSA), an intelligence agency within the Department of Defense (DoD). I am responsible for directing the NSA and overseeing the operations undertaken to carry out its foreign intelligence mission. One of my primary responsibilities is to collect signals intelligence (SIGINT) related to the activities of international terrorist groups and their agents, and to disseminate this intelligence information to a variety of intelligence consumers, including the FBI and CIA.

Derived From: NSA/CSSM 123-2
Dated: 24 Feb 1998
~~Declassify On: X1~~

1871 (c) (2) PRODUCTION JULY 2009 2357

(U) PURPOSE OF DECLARATION

2. (~~S//SI~~) I make this declaration in support of the Government's Application for Pen Register and Trap and Trace devices pursuant to the Foreign Intelligence Surveillance Act of 1978, 50 USC, sections 1801-1811, 1841-1846, as amended. As set forth in greater detail below, the surveillance authority requested will enable NSA to discover [redacted] and their communications, and to disseminate such information to support the efforts of the United States, and in particular the FBI, to detect and prevent terrorist acts against U.S. interests. This will be accomplished by collecting E-mail addressing [redacted] information (hereinafter meta data)[1]--not the contents of the communications--and then applying sophisticated algorithms to analyze meta data related to specific terrorist-associated E-mail addresses. 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, and (iv) the advice of counsel.

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

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

[1](~~S~~) Meta data is the information appearing on the "to," "from," "cc," and "bcc" lines of a standard E-mail [redacted] It does not include information from either the "subject" or "re" line of the E-mail, from the body of the E-mail [redacted]

1871 (c) (2) PRODUCTION JULY 2009 2358

[redacted]

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

[redacted]

(~~S//SI~~) AVAILABILITY OF INTERNET COMMUNICATIONS IN THE UNITED STATES

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

[redacted]

[2] (~~TS//SI~~) NSA statistics show that of the [redacted] total number of E-mail addresses in the NSA CounterTerrorism tracker database [redacted]

1871 (c) (2) PRODUCTION JULY 2009 2359

[redacted]

6. ~~(C)~~ [redacted]

[redacted]

[redacted]

[redacted]

[3](U) [redacted]

[4](U) [redacted]

[5](U) [redacted]

[redacted]

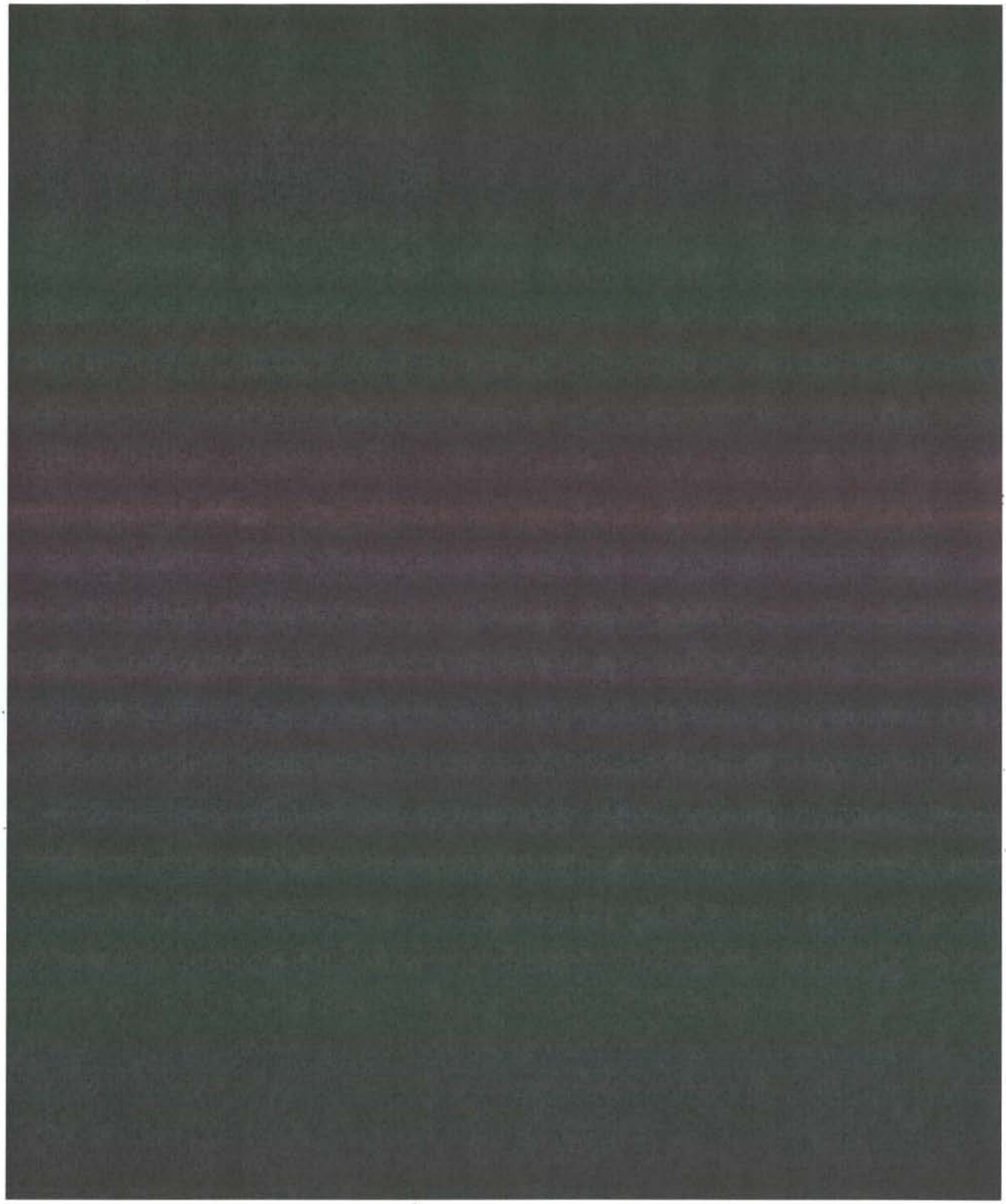
(S//SI) DATA NSA SEEKS TO ACCESS

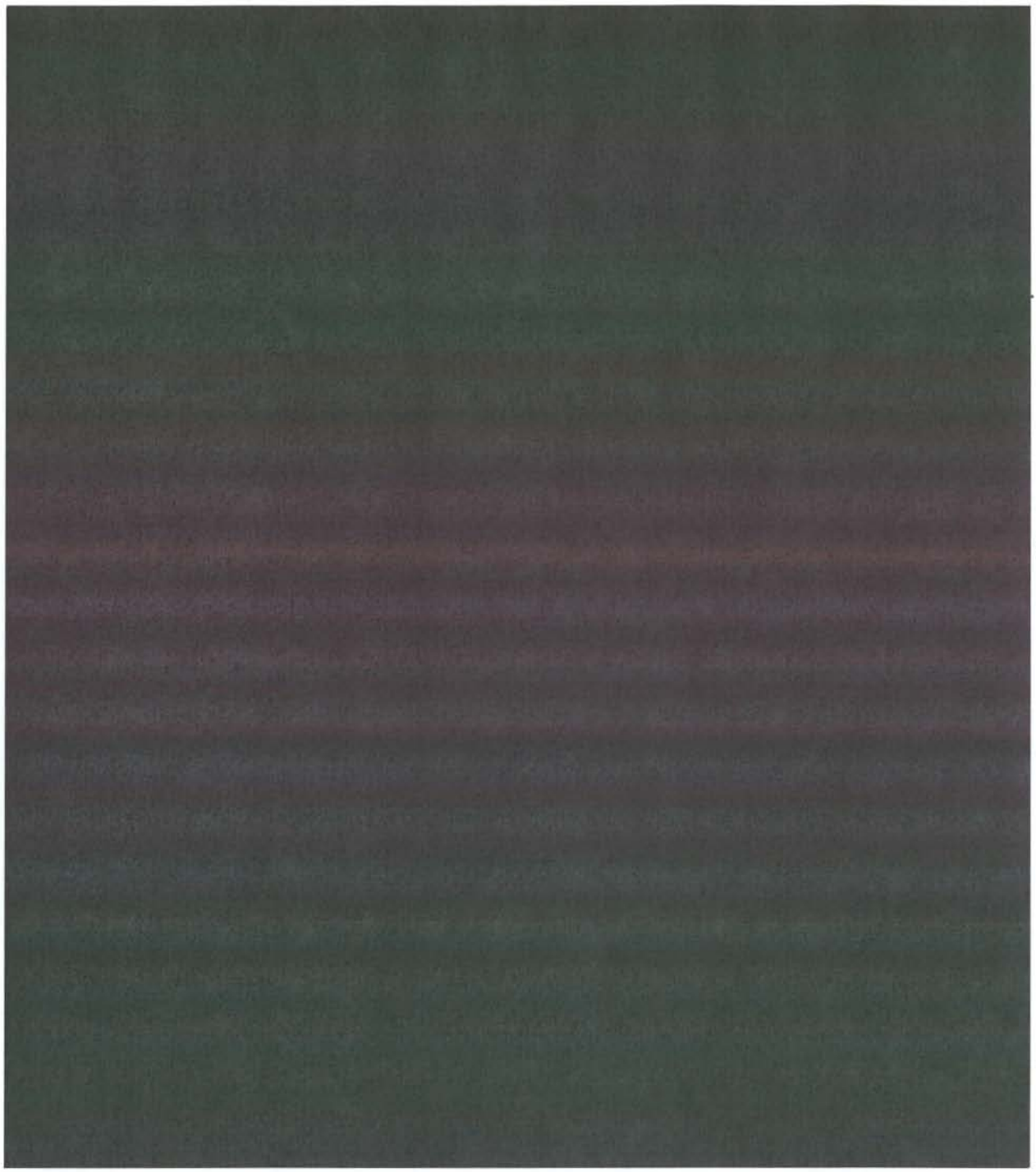
7. (TS//SI//NF) The accompanying Application seeks authority to obtain access to [redacted] that NSA has identified as relevant to ongoing terrorist investigations to detect and prevent hostile acts against U.S. interests. [redacted]

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

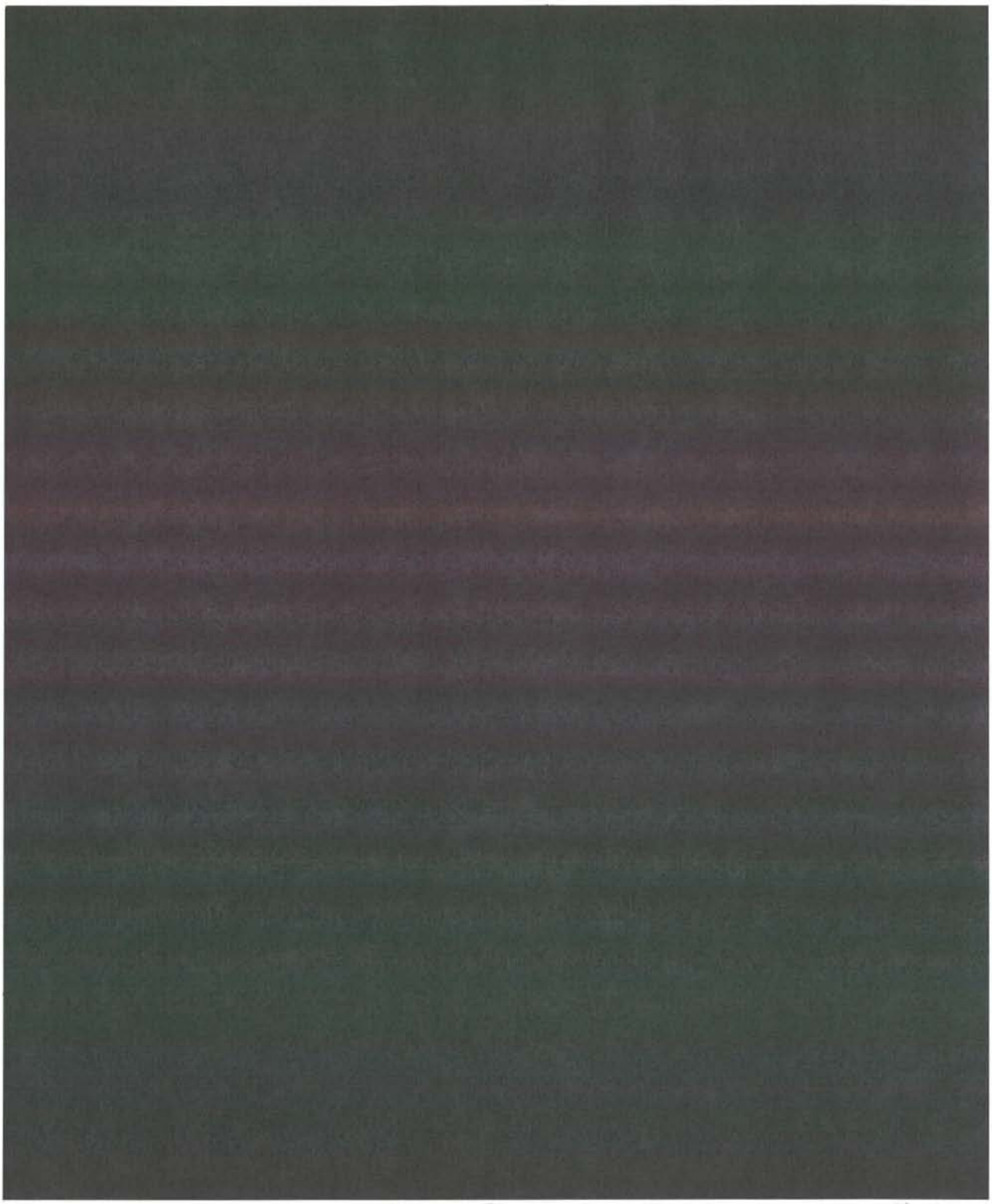
[6] (U//FOUO) This Declaration, the Application and the Memorandum of Law with which it is filed generically identify [redacted]

1871 (c) (2) PRODUCTION JULY 2009 2361

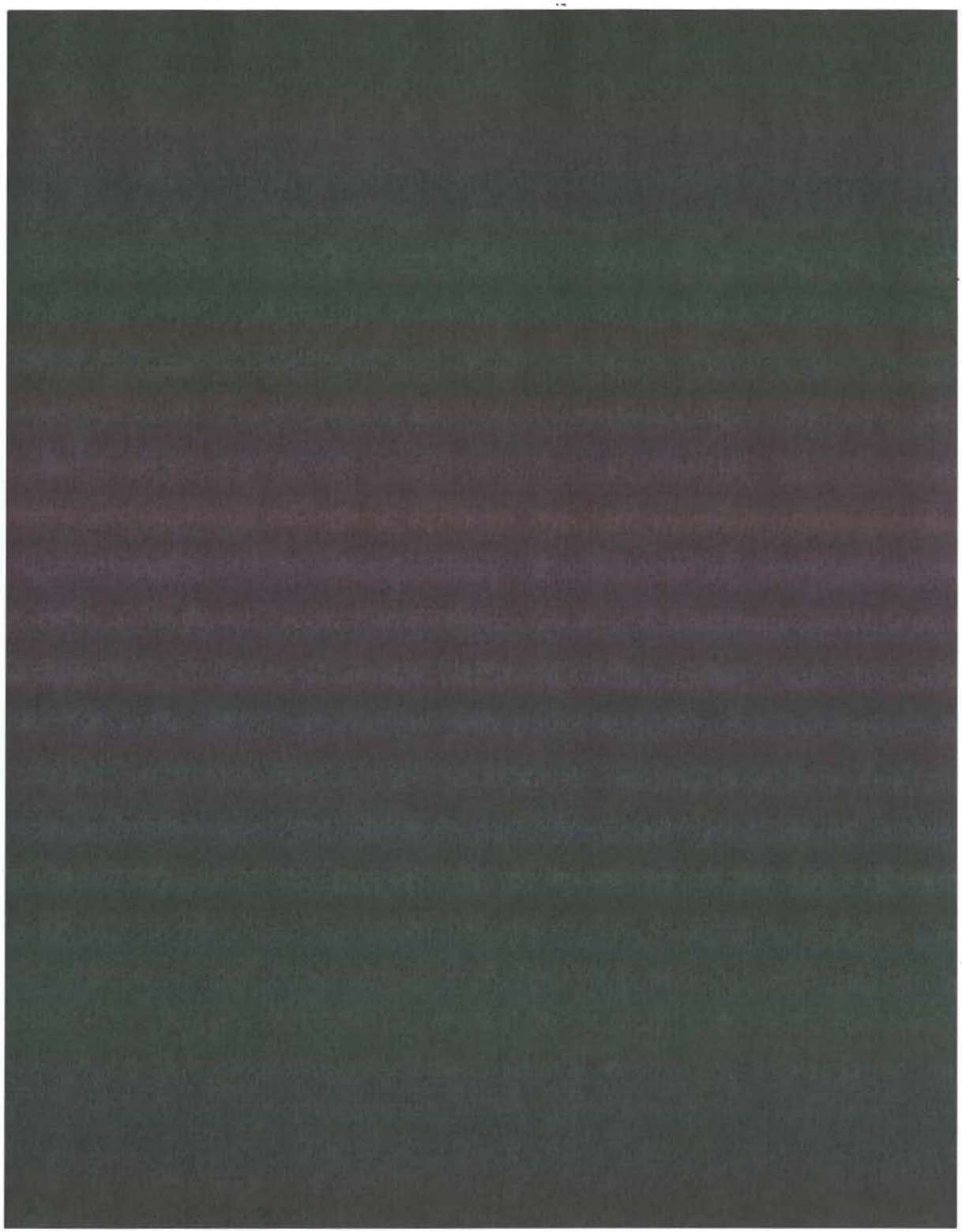


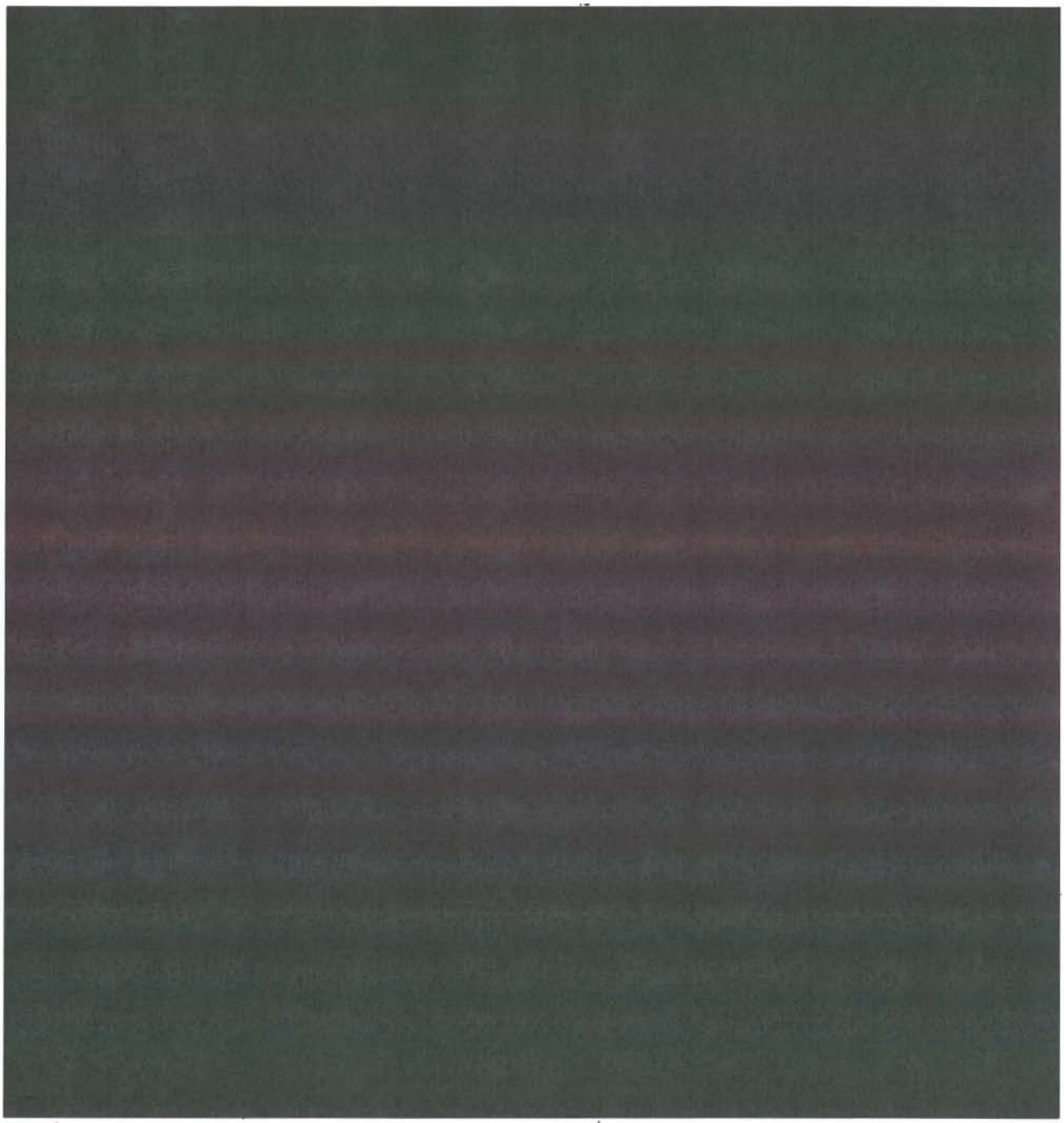


1871(c)(2) PRODUCTION JULY 2009 2363



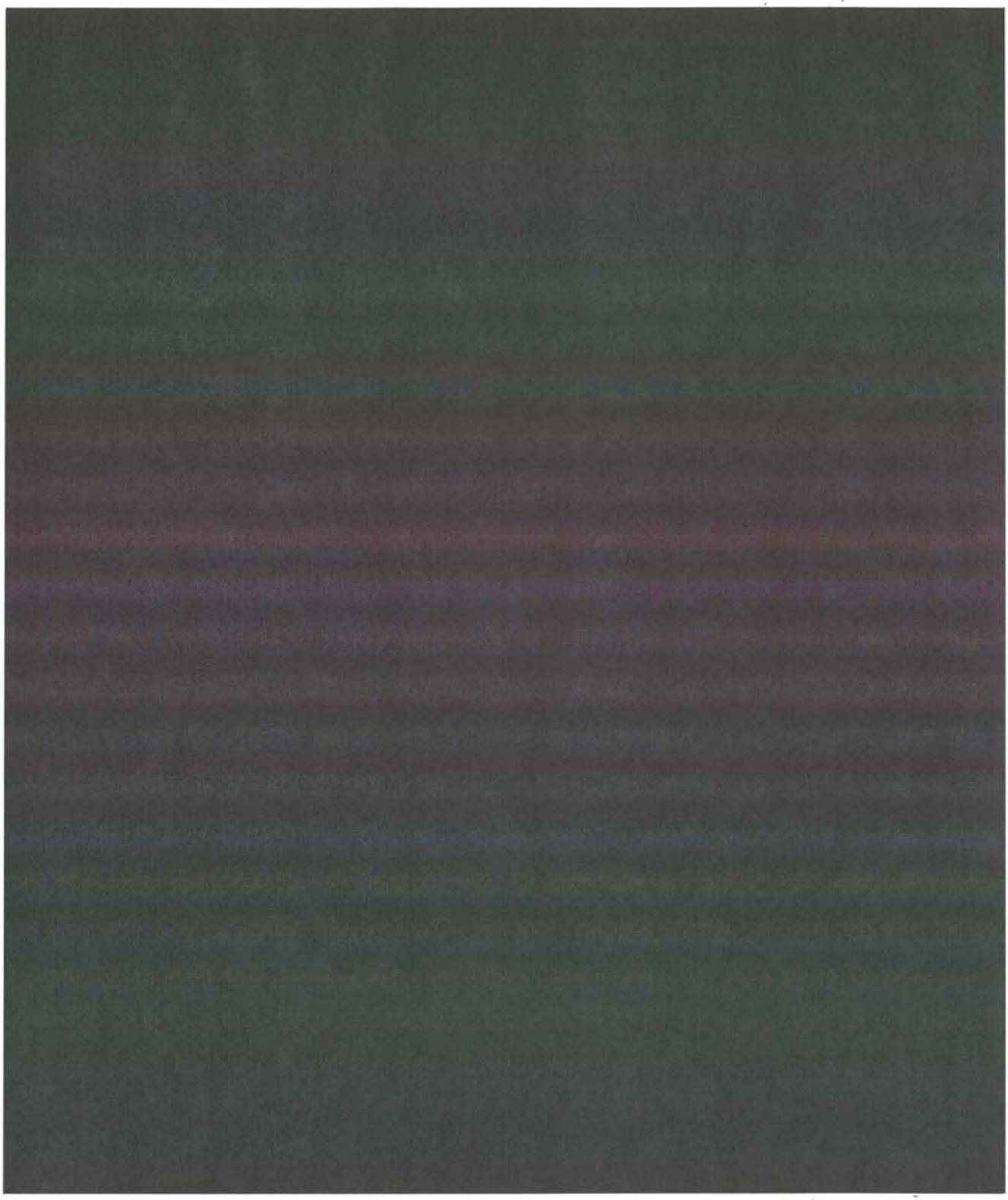
1871 (c) (2) PRODUCTION JULY 2009 2364





[redacted]

8 (S)



[redacted]

~~(S)~~ SMALL PROPORTION OF INTERNET BANDWIDTH NSA WILL OBTAIN

10. ~~(TS//SI//NF)~~ NSA estimates that if the Application is granted, it will routinely under this authority collect meta data associated with approximately [redacted] NSA estimated this percentage by computing the aggregate bandwidth of the access it seeks – approximately [redacted] – as a percentage of the approximately [redacted]

[redacted]

[9] (U) [redacted]

1871 (c) (2) PRODUCTION JULY 2009 2368

[redacted]

[redacted]

[11] (U) [redacted]

[redacted]

11. (~~TS//SI//NF~~) Carrying out similar calculations using the same techniques for the remaining [redacted] sought by NSA would add [redacted] to the total accumulated. Accordingly, we estimate that the [redacted] to which we seek access in the Application that this Declaration supports equates to approximately [redacted]

(~~C~~) WHY NSA SEEKS ACCESS TO THIS AMOUNT OF DATA

12. (~~TS//SI//NF~~) To better ensure success in its counterterrorism intelligence mission, NSA needs to have access to the accumulated pool of meta data described in the Application and this Declaration. By focusing through the various means described herein on countries of counterterrorism interest to NSA and on communications services known to be used by [redacted] NSA will attempt to limit the pool of data collected to that most likely to contain information about potential terrorism targets of interest. It is not possible, however, to target collection solely to known terrorist E-mail accounts and at the same time use the advantages of meta data analysis to discover the enemy. This is because [redacted] operatives take affirmative and intentional steps to disguise and obscure their

[12](~~S//SI~~) This estimate is, of necessity, rough, due to a number of factors. The measurement of total bandwidth [redacted] is not, of course, precisely equal to the capacity [redacted] Despite all of these facts, however, we believe the estimate is as precise as possible and is close to the mark.

1871 (c) (2) PRODUCTION JULY 2009 2370

communications and their identities. They do this using a variety of tactics, set out more fully below, [redacted] The only effective means by which NSA analysts are able to continuously keep track of [redacted] making use of such tactics is to obtain and maintain an archive of meta data that will permit these tactics to be uncovered. [redacted]

13. (~~S//SI~~) Because it is impossible to determine in advance which particular meta data will turn out to identify a terrorist, collecting meta data in the manner set out above is vital for success. To be able to fully exploit meta data, the data must be collected in bulk. Analysts know that the terrorists' E-mails are located somewhere in the billions of data bits; what they cannot know ahead of time is exactly where. If meta data is not collected by the Government at the time that E-mails are transmitted, that data disappears and is lost forever and with it potential opportunities to prevent catastrophic events.

14. (~~TS//SI//NF~~) The ability to accumulate a meta data archive and set it aside for carefully controlled searches and analysis will substantially increase NSA's ability to detect and identify members of [redacted] The NSA will be able to perform [redacted] queries on the database: contact-chaining, to determine the contacts made by a particular terrorist-associated E-mail account, [redacted] described below.

15. (~~TS//SI//NF~~) When the NSA performs a contact-chaining query on a known terrorist-associated account, computer algorithms will identify all the contacts made by that account and also will automatically identify the further contacts made by that first tier of contacts. The archive will thus hold contact

1871 (c) (2) PRODUCTION JULY 2009 2371

information that can be immediately tapped as new terrorist-associated addresses are identified.

16. (~~TS//SI//NF~~) To some extent, archived information can be historical in nature, reflecting contact activity from the past that cannot be captured in the present. In addition, meta data flows into the archive may also be very timely and well suited for alerting against suspect activity. To the extent that historical connections are important to understanding a newly-identified target, extracted meta data may contain links which are absolutely unique, pointing to potential targets that otherwise would be missed. [redacted]

17. (~~TS//SI//NF~~) When NSA makes a contact-chaining query to the archive on a terrorist-associated account, the query will also return meta data [redacted]. [redacted] This information is important because [redacted]

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

1871 (c) (2) PRODUCTION JULY 2009 2372

[redacted]

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

[redacted]

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

1871 (c) (2) PRODUCTION JULY 2009 2373

[redacted]

21. (~~S//SI~~) Were NSA to use pen registers targeted individually at specific terrorist-associated E-mail [redacted] to collect the E-mail addresses in contact [redacted] and the E-mail addresses in contact with the first-tier of E-mail addresses, i.e., going "two hops out"—a process that would entail approximately [redacted] pen register applications per year,[14] NSA would acquire approximately [redacted] of all the E-mail addresses that would be collected by the [redacted] if the current Application were granted. [redacted]

(U) INTERNAL CONTROLS/MINIMIZATION PROCEDURES

22. (~~TS//SI//NF~~) I will establish mandatory procedures to strictly control access to and use of the archived data collected pursuant to an order of this Court. First, any search or analysis of the data archive will occur only after a particular E-mail address has been associated with [redacted]

[redacted]

[14] (~~TS//SI//NF~~) This calculation is based on the estimate that there are [redacted] "seed" addresses that warrant a pen register and that each of those [redacted] addresses is in contact with an average of [redacted] other E-mail addresses.

1871 (c) (2) PRODUCTION JULY 2009 2374

[redacted] More specifically, access to the archived data will occur only when, 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 E-mail address is associated with [redacted] All query activity will be recorded by the interface to the meta data archive for auditing purposes. The controls I will institute are set out more fully below.

23. (~~TS//SI//NF~~) NSA will obtain the meta data from the above-referenced providers of wire or electronic communications services [redacted] The meta data will be stored and processed on a secure private network that NSA exclusively will operate. NSA will restrict access to the private network to two administrative login accounts used exclusively by personnel cleared especially for this program. The NSA private network will be accessible via select machines, and only be accessible to cleared system administrators, using secure encrypted communications. The data will reside on dedicated servers and will not be commingled with data collected pursuant to other authorities. The datasets will be password protected and access to them will be restricted. When the datasets are accessed, the user's login, IP address, date and time, and retrieval request will be logged for auditing capability.

24. (~~TS//SI//NF~~) Access to the meta data archive will be accomplished through a software interface which will limit access to this data to authorized analysts. NSA currently plans to have ten analysts perform such queries on a regular basis, although that number may vary in the future. Access to the archive will be controlled by user name and password. Analysts will be briefed by NSA's Office of General Counsel concerning the authorization requested in this application and the limited circumstances in which queries to the archive are permitted.

25. (~~TS//SI//NF~~) Although the data collected under the attached Application will necessarily be broad in order to achieve the critical intelligence objectives of meta data analysis, the use of that information for analysis will be strictly tailored

to identifying terrorist communications and will occur solely according to stringent procedures, including minimization procedures designed to protect U.S. person information. Specifically, collection minimization will be carried out by focusing almost exclusively on [redacted] Dissemination minimization will follow the standard NSA minimization procedures found in USSID 18. Before information identifying a U.S. person may be disseminated outside of NSA, a judgment must be made that the identity of the U.S. person is necessary to understand the foreign intelligence information or to assess its importance. Prior to the dissemination of any U.S. person identifying information, the Chief of Customer Response in the Signals Intelligence Directorate 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. A record is made of every such determination.

26. (~~TS//SI//NF~~) Fewer than one new lead (i.e., E-mail address for which there is a reasonable articulable suspicion that the address is associated with [redacted] is expected to be obtained daily from a combination of external intelligence sources and from NSA's own internal analysis. Each lead, when pursued via the database, can be expected to generate, on average, [redacted] addresses one level out and [redacted] addresses two levels out, with which the original E-mail address has had contact. This number is then reduced significantly using analytic tradecraft, resulting in roughly 400 E-mail addresses being tipped to FBI and CIA every year, or an average of just over one per day. Typically, a very low proportion of the results of the searches would include U.S. person information. Approximately 25 percent of all E-mail addresses tipped to the FBI and the CIA would include U.S. person information. Based on the number of expected leads, that would amount to information regarding approximately four to five U.S. persons each month.

1871 (c) (2) PRODUCTION JULY 2009 2376

27. (~~C~~) The collected meta data will be kept online (that is, accessible for queries by cleared analysts) for only 18 months, at which time it will be transferred to a tape system that is inaccessible to software tools and queries from analysts. If data older than 18 months old is needed in a specific case, the tape library will be searchable only by a cleared administrator.

28. (~~TS//SI//NF~~) Internal management control will be maintained by requiring that queries of the archived data be approved by one of seven persons: the Program Manager, Counterterrorism Advanced Analysis; Chief or Deputy Chief, Counterterrorism Advanced Analysis Division; or the Counterterrorism Advanced Analysis Shift Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate.

29. (~~TS//SI//NF~~) The Program Manager, Counterterrorism Advanced Analysis; Chief and Deputy Chief, Counterterrorism Advanced Analysis Division; and Counterterrorism Advanced Analysis Shift Coordinators will be required to establish appropriate management controls (e.g., records of all tasking decisions, audit and review procedures) for access to the archived data and shall use the Attorney General approved guidelines (USSID 18) to minimize the information reported concerning U.S. persons.

30. (~~TS//SI//NF~~) The NSA Inspector General, the NSA General Counsel and the Signals Intelligence Directorate Oversight and Compliance Office will periodically review this program. The Inspector General and the General Counsel will submit a report to me forty-five days after the initiation of the collection activity assessing the efficacy of the management controls and ensuring that any dissemination of U.S. person information has been accomplished in accordance with the USSID 18 procedures.

1871 (c) (2) PRODUCTION JULY 2009 2377

31. (~~TS//SI//NF~~) Also, in coordination with the Attorney General, I will inform the leadership of the Congressional Intelligence Oversight Committees of the Court's approval of this collection activity.

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

Signed this [redacted]

Michael V. Hayden

MICHAEL V. HAYDEN
Lieutenant General, USAF
Director, National Security Agency

1871 (c) (2) PRODUCTION JULY 2009 2378