Description of document:	US Privacy and Civil Liberties Oversight Board (PCLOB) Report on NSA Activities (Deep Dive), 2020
Source of documents:	US Privacy and Civil Liberties Oversight Board (PCLOB)
Accessed date:	21-December-2025
Posted date:	30-December-2025

US PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

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

Privacy and Civil Liberties Oversight Board

Report on Certain NSA Uses of XKEYSCORE for Counterterrorism Purposes

December 2020

Privacy and Civil Liberties Board • PCLOB.gov • info@pclob.gov

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

Classified By: Privacy and Civil Liberties Oversight Board
Derived From: Multiple Sources
Declassify On: 20461231

Board Members

Adam I. Klein, Chairman
Edward W. Felten
Jane E. Nitze
Travis LeBlanc
Aditya Bamzai

The Board acknowledges with gratitude the staff members who have worked on this project, including Paige Anderson, Matthew Eldred, Joel Todoroff, Board Counselors, and other current and former staff members.

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

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Table of Contents

I. (U) Introduction

A. (U) The Board's Examination of Executive Order 12333 Activities

(U) In July 2014, the Board announced that it would review, among other matters, counterterrorism-related intelligence activities conducted pursuant to Executive Order 12333 ("E.O. 12333").[1] First issued in 1981 and last updated in 2008, E.O. 12333 establishes an operational framework for 17 federal entities designated as part of the nation's Intelligence Community ("IC").[2] The executive order does not provide authority for any one intelligence-gathering effort, nor is there any single E.O. 12333 surveillance "program." Nonetheless, understanding how IC elements implement E.O. 12333 is a critical part of understanding how they protect privacy and civil liberties while also protecting the nation against terrorism.

(U) The executive order regulates the use of certain intelligence-gathering methods and outlines parameters under which intelligence agencies may collect and utilize information about United States persons ("USPs"). Among other things, E.O. 12333 requires IC elements to follow procedures approved by the Attorney General in order to collect, retain, or disseminate information concerning USPs, or to use certain collection methodologies within the United States or directed at USPs abroad.[3]

United States Persons

(U) A "United States person" under E.O. 12333 means (1) "a United States citizen," (2) "an alien known by the intelligence element concerned to be a permanent resident alien," (3) "an unincorporated association substantially composed of United States citizens or permanent resident aliens," or (4) "a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." E.O. 12333 § 3.5(k).

(U) In April 2015, the Board adopted a project description memorializing its E.O. 12333 oversight effort. The Board explained that it would select specific counterterrorism-related activities conducted under E.O. 12333 by the National

---

[1] (U) Executive Order No. 12,333 (hereinafter E.O. 12333).

[2] (U) E.O. 12333 was signed on December 4, 1981. It was amended in 2004 by Executive Order 13355 to facilitate "strengthened management of the Intelligence Community." E.O. 12333 was again amended in 2008 by Executive Order 13470 to strengthen the role of the Director of National Intelligence and permit the sharing of signals intelligence under certain conditions.

[3] (U) E.O. 12333 §§ 2.3-2.4.

Security Agency ("NSA") and Central Intelligence Agency ("CIA"), and would conduct in-depth examinations of those activities. The Board also stated that it would issue a public report on the legal framework that governs the collection, use, retention, and dissemination of information concerning USPs.[4] In November 2015, the Board approved a project description for NSA review. That project description focused the Board's efforts on an NSA activity conducted using the Agency's processing and discovery system known as XKEYSCORE. Throughout 2016, Board staff prepared draft documents and ultimately created an interim statement of facts and recommendations. By the time this was complete, the Board had become inquorate, and the report could not be finalized. Nonetheless, the interim statement of facts and the recommendations were shared with NSA to confirm their accuracy.[5] In turn, NSA shared the interim statement of facts with the Department of Justice.

(U) When the sub-quorum period ended in late 2018, the Board began reviewing work done previously and sought to bring pending projects to an appropriate conclusion. In early 2019, the Board renewed its efforts to complete the report on XKEYSCORE.

B. (U) Focus and Purpose of This Report

(~~S//REL TO USA, FVEY~~) The focus of this report is XKEYSCORE as used to support NSA's E.O. 12333 signals intelligence ("SIGINT") mission.[6]

---

4 (U) "PCLOB Examination of E.O. 12333 Activities in 2015," *available at* https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf.

5 (~~TS//SI//REL TO USA, FVEY~~) These included recommendations to harmonize the governing policy documents with existing privacy-protective practices, and to track and minimize how much US person information XKEYSCORE processes. NSA did not formally adopt any of these recommendations, and the Board reiterates some of them below.

6 (U) According to NSA, SIGINT comprises communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, either individually or in combination. Communications intelligence ("COMINT") is defined as "technical and intelligence information derived from foreign communications by other than the intended recipients" and "the collection and processing of foreign communications passed by radio, wire, or other electromagnetic means." *See* NSCID 6 § 4(b). *See also* NSA/CSS Policy 1-23.

(~~TS//SI//REL TO USA, FVEY~~) As described in more detail below, XKEYSCORE is a processing and discovery system used with NSA's collection architecture. XKEYSCORE is a tool [redacted] and not a discrete intelligence "program." XKEYSCORE's capabilities are diverse and powerful, but, at a high level, XKEYSCORE is used to process [redacted] traffic acquired pursuant to E.O. 12333.[7] In the counterterrorism context, NSA uses XKEYSCORE for identifying new terrorism-related targets and selectors, methods of communications used by terrorists [redacted].

SIGINT

(U) SIGINT is intelligence derived from electronic signals and systems such as communications networks, radars, and weapons systems. It includes communications between people and electronic signals that are not directly used in communications, such as automated machine-to-machine data flows.

(~~S//SI//REL TO USA, FVEY~~) XKEYSCORE's technical capabilities are broad. NSA uses these capabilities in a number of different ways, for both counterterrorism activities and other foreign intelligence objectives, such as gathering foreign military and political information and identifying the activities of foreign intelligence services.[8] Given the diversity of XKEYSCORE's capabilities, the Board focused on aspects that are uniquely powerful and most directly implicate USP privacy and civil liberties. These aspects included NSA's choices about [redacted] and how NSA analysts access and index that data. Accordingly, this report does not comprehensively examine all aspects of XKEYSCORE's capabilities.[9]

---

[7] (~~S//SI//REL TO USA, FVEY~~) NSA refers to this as [redacted] typically by way of signals intelligence collection.

[8] (~~S//REL TO USA, FVEY~~) The Board has focused on the use of XKEYSCORE for counterterrorism purposes. However, XKEYSCORE is used in the same way, or similar ways, for other foreign intelligence activities. Thus, the Board believes this report is applicable to a range of NSA activities utilizing XKEYSCORE—not just those aspects relating to counterterrorism.

[9] (~~S//REL TO USA, FVEY~~) For example, the capabilities in XKEYSCORE allow for [redacted] But these capabilities were not part of the Board's examination because they do not raise novel privacy and civil liberties questions in the same way that XKEYSCORE's search-and-discovery capabilities do. For more on how the Board focused its examination, see the criteria outlined in the Board's announcement of its E.O. 12333 investigations. "PCLOB Examination of E.O. 12333 Activities in 2015," *available at* https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(~~S//REL TO USA, FVEY~~) This report examines these aspects of XKEYSCORE in light of the privacy and civil liberties implications they raise for USPs. The Board believes this report will advance the understanding for appropriately cleared individuals of XKEYSCORE's critical capabilities and their impact on privacy and civil liberties. In addition, the Board offers recommendations for how NSA and other entities can responsibly balance mission needs against U.S. persons' privacy and civil liberties as XKEYSCORE and the broader technological environment evolve.

C. (U) Methodology

(U//~~FOUO~~) The Board's initial oversight was informed by briefings and other discussions between NSA and Board Members and staff between May 2015 and November 2016. The Board reviewed guidance and training provided to NSA personnel, oversight and compliance mechanisms, and the relationship between XKEYSCORE and NSA's E.O. 12333 implementing procedures. The Board also received relevant documents from NSA, including policies, training materials, manuals, and handbooks. After the Board regained a quorum, the Board reengaged with NSA and received additional briefings, demonstrations, and information. The Board worked with NSA to reconfirm the validity of facts and briefings that were provided in the 2015 timeframe.

[redacted]

(~~S//FOUO~~) Section II starts by describing technical concepts related to the internet in general, then gives an overview of XKEYSCORE. These technical concepts [redacted] Section III starts with [redacted] collection that determines what data goes into XKEYSCORE. Then it provides a deeper look at XKEYSCORE as a processing and discovery system. Section IV describes NSA's explanations of its authorities and legal limitations. Section V makes recommendations to NSA.

II. (U) Overview: The Internet [redacted]

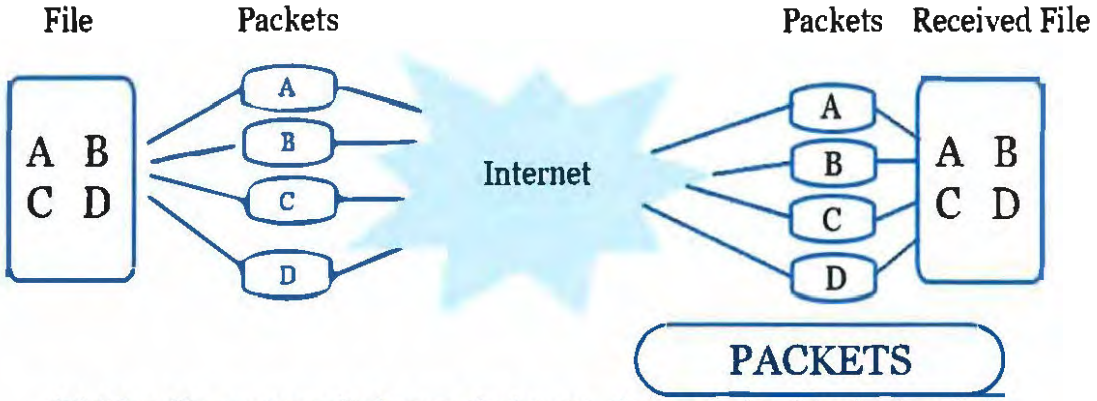
A. (U) The Internet

(U) When browsing the internet—say, going to Google to look up a fact or Netflix to watch a show—many take for granted that they can type in www.google.com or www.netflix.com, the page will appear, and soon thereafter the facts or show they were intending to browse will also appear. This sequence of events happens so quickly that one may assume that the processes underlying it are straightforward. They are not.

(U) When a user enters the name of a website (i.e., the URL) into a browser, the computer does not initially know how to contact that website. Indeed, it does not know what "Wikipedia" or "Netflix" or "Google" is, never mind how to connect to it. To view a website, the address, like www.google.com, is first translated into a numeric internet protocol ("IP") address—a series of decimal or hexadecimal numbers that corresponds to the server providing the webpage.[10] Information the user is sending, such as a request for a website, is then sent in "packets," which are pieces of digital communications (web page requests, emails, internet-based telephony, etc.) that contain both the user's IP address as well as the IP address of the remote machine with which they are communicating.

[10] (U) These IP addresses are obtained through the "domain name system" ("DNS"). JAMES F. KUROSE & KEITH W. ROSS, COMPUTER NETWORKING: A TOP-DOWN APPROACH § 2.4 (7th ed. 2017). The network graphic on page 8 is also from this textbook.

(U)



(U) When files are transmitted across the internet, they are broken into chunks, called packets, which are individually routed to the final destination and reassembled when they get there.

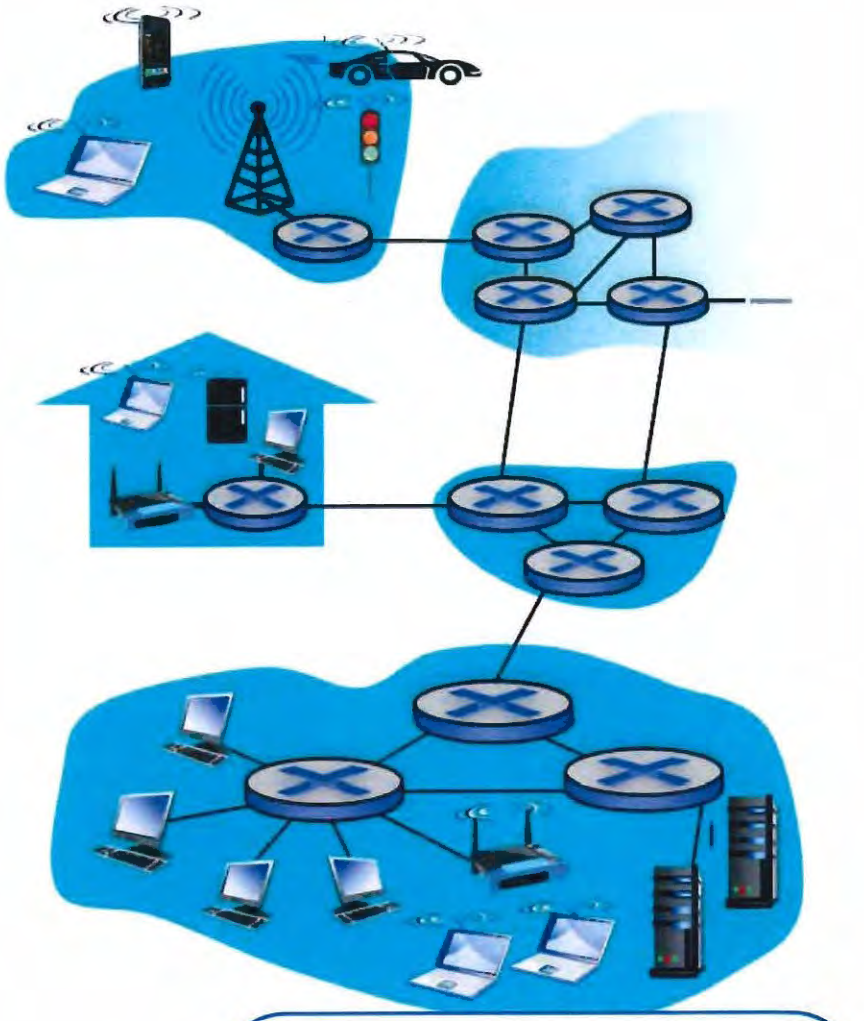
(U)

(U) Similarly, even when the user's computer knows the IP address to which the packets should go, it generally does not know how to get the packets there. Instead, the packets are sent to a piece of hardware—a router—which contains more information on where to direct packets based on their destination IP. Often, there is another router. Thus, a commercial router may not direct an office's internal packets to their destination, but rather direct traffic to and from the broader internet to a router belonging to an internet service provider (ISP). In turn, that router will check to see if it knows where to route the packets and will continue the process. For example, the ISP may not be able to fully route the packets because it is not connected to the final destination; the ISP instead will direct them to another router it believes is closer to the destination and will know how to route the packets—say that of a different ISP. That ISP, in turn, may know that the IP address belongs to a commercial enterprise it services, and direct the packets to that router. That router will know the specific device to communicate with, and deliver the packets to their final destination. This process would be repeated in the reverse direction as packets are sent back.

(U) The path that packets take to travel between destinations need not be tightly correlated to the locations of the participants. In an attempt to communicate online with a person in the same city, it is possible the packets would travel hundreds or thousands of miles away before returning. It generally makes sense to limit needless data movement, but the router that knows how to find a neighbor may not be in that neighborhood, or even in that city. Moreover, routing decisions are based, in part, on the agreements companies make with each other and the cost of moving that data. Thus, even if there is a fairly direct connection between two systems, an ISP may determine it is more cost effective to use a different router in a different location to direct the data.

(U) Movement along these routes generally occurs through physical cables. This is true for most of a packet's travel, even if a user is connected to the internet via a wireless or a cellular connection. This is because in most cases, as noted above, when a smartphone or laptop user is browsing the internet, their device is not connected directly to the server hosting that internet content. Rather, the user's device is first connected, via wireless internet or a cellular connection, to a piece of hardware located nearby, often a home or business router. However, a physical cable often connects that router to a broader network, such as one owned by an ISP. These are, in turn, generally connected to other networks via physical cables. Thus, the communications between two people on laptops, both connected wirelessly to the internet, are extremely likely to pass through a series of physical cables.

(U)



(U)

(U) The paths taken by packets sent from address A to address B may vary over time, even from minute to minute, and the path taken from A to B may not be the exact reverse of the path from B to A. Network routes can and do change in real time to route around network failures or traffic congestion.

(U) Today, the world is crisscrossed with those cables, which are responsible for carrying the vast majority of digital communications. This includes undersea cables, often operated by private companies that engage in agreements with peers and service providers for the transmission of communications worldwide.[11] It also includes cables running to homes, schools, and businesses. The physical cables around the world thus move huge volumes of data: data destined to or from people who may live or work by one of those cable's terminal points and, potentially, data to or from people in other parts of the world, who have their data routed through the cable as one of many steps on a longer path.

(U)

SUBMARINE CABLES IN ASIA

(U)

(U) As the need to pass this digital information has increased, so too has the bandwidth (a measure of the capacity of data transfer) of these cables. Modern cables

[11] (U) *See, e.g.*, Undersea Cables Transport 99 Percent of International Data, *Newsweek* (Apr. 2, 2015), *available at* www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072.

now use fiber optics to transmit digital information. To maximize the amount of data that can be transferred, a cable may bundle together multiple fibers. Each of those fibers is actually capable of carrying multiple communications simultaneously as distinct wavelengths, each referred to as a "communications link."[12]

(U) This means the cables carrying web browsing, Netflix shows, email communications, or voice traffic are neither directly between a user and, say, Netflix, nor are they exclusively the user's. Someone's packets may be passing through cables hundreds of miles away alongside the emails or Netflix queue of a stranger they have never met. This process is largely invisible, almost instantaneous, and, for most internet users, completely unnecessary to understand.

B. (U) NSA Activities

(~~TS//SI//REL TO USA, FVEY~~)

to enable NSA's intelligence-gathering mission. That mission is guided by intelligence requirements set by policymakers to inform US government objectives, including counterterrorism.

(~~TS//SI//REL TO USA, FVEY~~)

NSA conducts target development and discovery. These activities could include

(~~TS//SI//REL TO USA, FVEY~~)

[redacted]

[12] (~~U//FOUO~~) NSA Brief for PCLOB, Slide 15 (May 27, 2015).

[13] (U) As directed by the President under E.O. 12333.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(~~TS//SI//REL TO USA, FVEY~~) [redacted]

[redacted]

(U) None of that is XKEYSCORE, the subject of the Board's review and this report. XKEYSCORE begins with what NSA does next.

(~~TS//SI//REL TO USA, FVEY~~) [redacted]

[redacted]

(~~TS//SI//REL TO USA, FVEY~~) [redacted]

[redacted]

---

[14] (~~TS//SI// REL TO USA, FVEY~~) [redacted]

[redacted]

[15] (~~S//REL TO USA, FVEY~~) [redacted]

[redacted]

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(~~TS//SI//REL TO USA, FVEY~~)

(~~TS//SI//REL TO USA, FVEY~~)

(~~TS//SI//REL TO USA, FVEY~~)

[16] (~~S//SI//REL TO USA, FVEY~~)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

III. (U) XKEYSCORE in Depth

A. (~~C//REL TO USA, FVEY~~) Determining What Data Goes into XKEYSCORE

(~~TS//SI//REL TO USA, FVEY~~) The activities we have reviewed involve the use of XKEYSCORE as a data analysis tool rather than a data collection system. Therefore, before NSA uses XKEYSCORE, it must decide what data to collect and send to XKEYSCORE

(~~TS//SI//REL TO USA, FVEY~~)

(~~TS//SI//REL TO USA, FVEY~~)

[redacted]

[17] (U//~~FOUO~~) NSA [redacted] Brief for PCLOB (May 27, 2015).

[18] (U//~~FOUO~~) PCLOB Notes from May 27, 2015 and July 23, 2015 NSA Briefings (with accuracy edits from NSA).

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(TS//SI//REL TO USA, FVEY)

(TS//SI//REL TO USA, FVEY)

(TS//SI//REL TO USA, FVEY)

(TS//SI//REL TO USA, FVEY)

(U//FOUO) NSA, Brief for PCLOB (Follow-up), Slide 5 (June 10, 2015).

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

(~~TS//SI//REL TO USA, FVEY~~) [redacted]

[redacted]

(~~TS//SI//REL TO USA, FVEY~~) [redacted]

[redacted] NSA tries to focus its collection on [redacted] that will provide the greatest amount of foreign intelligence on the most pressing intelligence priorities.[22]

(~~S//SI//REL TO USA, FVEY~~) [redacted]

[redacted]

(~~S//SI//REL TO USA, FVEY~~) [redacted]

[redacted] How NSA prioritizes foreign intelligence, and *de facto* deprioritizes USP and valueless data, evolves continually. But the goal is always to target and increase its

---

[20] (U//~~FOUO~~) NSA Briefing on XKEYSCORE (Feb. 7, 2019).

[21] (~~S//REL TO USA, FVEY~~) [redacted]

[redacted]

[22] (~~S//REL TO USA, FVEY~~) NSA [redacted] Brief for PCLOB, Slide 15 (May 27, 2015). [redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

collection of foreign intelligence and decrease its collection of "superfluous" data.[23] In 2015, when the Board began its XKEYSCORE review, NSA used [redacted] to exclude superfluous data.[24] As of 2020, when the Board requested updated information, [redacted] has become less common. Now, NSA uses improved [redacted] to prioritize retention of foreign intelligence traffic and delete unknown and superfluous traffic.[25] For example, [redacted]

~~(S//SI//REL TO USA, FVEY)~~ [redacted]

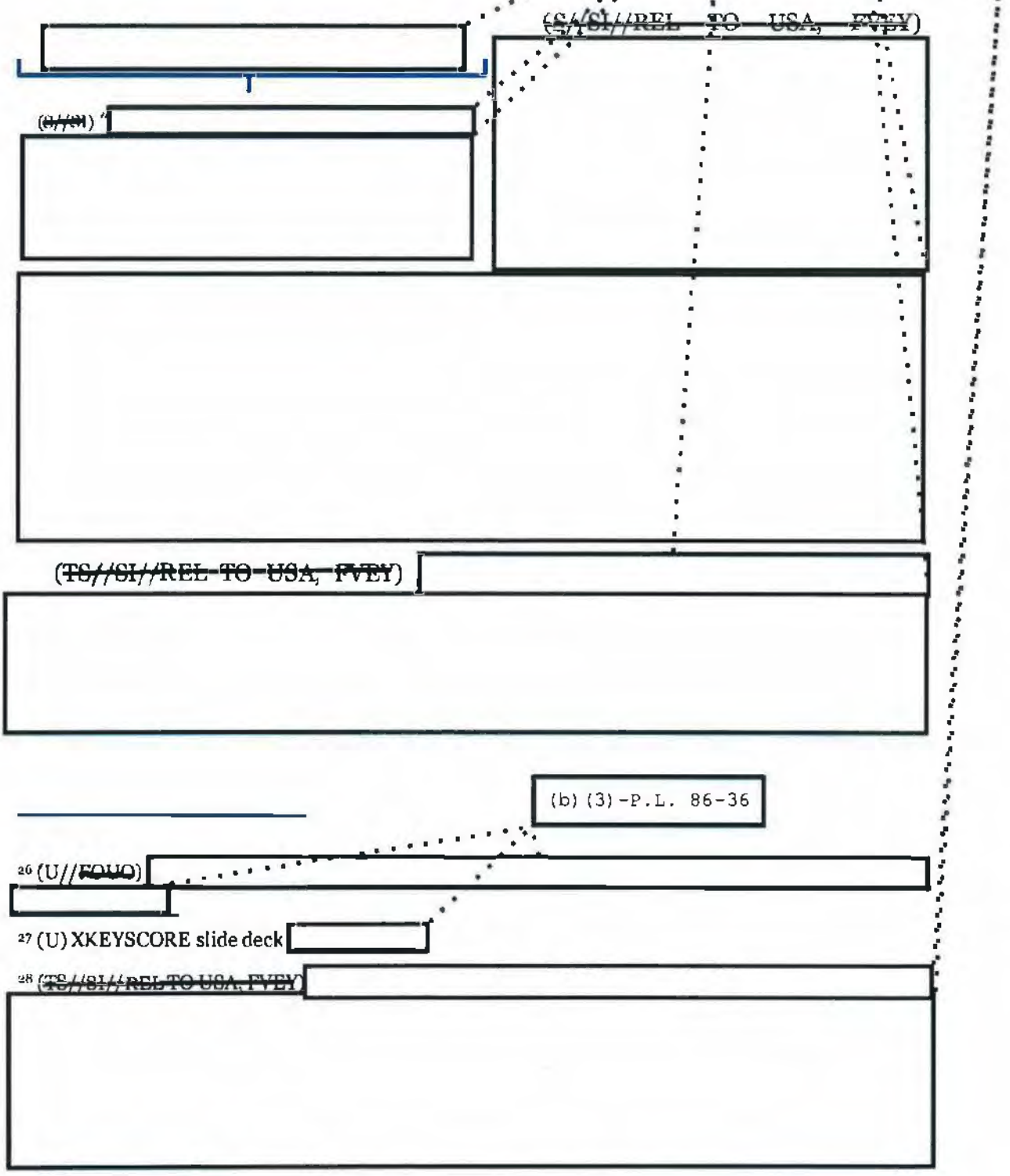
[23] ~~(S//REL TO USA, FVEY)~~ The Board understands "superfluous" data to mean valueless (USP or non-foreign intelligence) traffic.

[24] ~~(S//SI//REL TO USA, FVEY)~~ [redacted] *See* NSA response to notes from XKEYSCORE and survey and access briefings. *See also* Call with NSA re: Initial Answers to 2019 Tranche One PCLOB Questions (July 9, 2019).

[25] ~~(S//SI//REL TO USA, FVEY)~~ [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

B. (U//~~FOUO~~) XKEYSCORE as a processing and analysis tool



[26] (U//~~FOUO~~)

[27] (U) XKEYSCORE slide deck

[28] (~~TS//SI//REL TO USA, FVEY~~)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(~~TS//SI//REL TO USA, FVEY~~)

1. (U//~~FOUO~~) XKEYSCORE as System

(~~TS//SI//REL TO USA, FVEY~~)

[29] (~~TS//SI//REL TO USA, FVEY~~)

Phone call between NSA staff and PCLOB staff regarding NSA Deep Dive Follow-up Questions (Aug. 26, 2016).

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

[31] (U//~~FOUO~~) PCLOB Notes from May 27, 2015 and July 23, 2015 NSA Briefings (with accuracy edits from NSA).

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

NSA Answers to 2019 Tranche One PCLOB Questions (July 12, 2019).

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]

~~(TS//SI//REL TO USA, FVEY)~~ [redacted]

[redacted]

2. (U//~~FOUO~~) XKEYSCORE Processing and Indexing

(b) (3)-P.L. 86-36
(b) (5)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (5)

[33] (~~S//NF~~) [redacted] Legal Analysis of XKEYSCORE, p.4.

[34] (U//~~FOUO~~) NSA briefing on XKEYSCORE and Processing (July 23, 2015; follow-up briefing on Aug. 4, 2015).

[35] (~~S//SI//REL TO USA, FVEY~~) NSA response to notes from XKEYSCORE and survey and access briefings; *see also* NSA Legal Analysis of XKEYSCORE at n. 9 [redacted]

[36] (~~S//NF~~) *See* NSA Legal Analysis of XKEYSCORE, pp.9-10 [redacted]

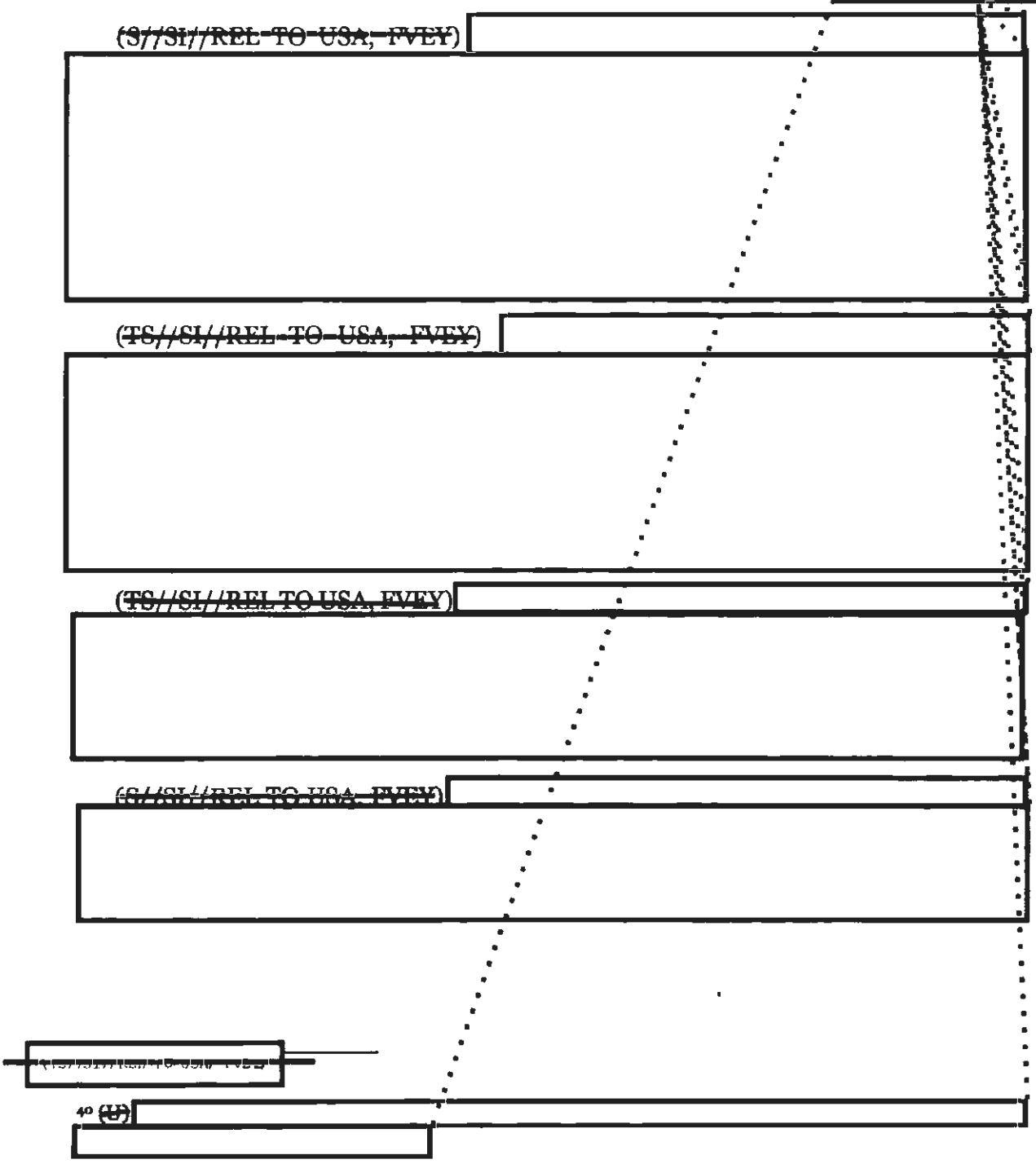
[37] (U//~~FOUO~~) Call with NSA re: Initial Answers to 2019 Tranche One PCLOB Questions (July 9, 2019).

[38] (U//~~FOUO~~) NSA Briefings and Demonstrations for the Board re: XKEYSCORE (Apr. 5, 2019).

[39] (U) NSA Answers to PCLOB Questions (Aug. 6, 2019).

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



[redacted]

40 (U) [redacted]

41 (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

42 (U) [redacted] (b) (3)-P.L. 86-36

43 (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

44 (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(~~S//SI//REL TO USA, FVEY~~)

(~~S//SI//REL TO USA, FVEY~~)

---

45 (~~S//REL TO USA, FVEY~~) *See* NSA response to notes from XKEYSCORE and survey and access briefings.

46 (~~TS//SI//REL TO USA, FVEY~~)

47 (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

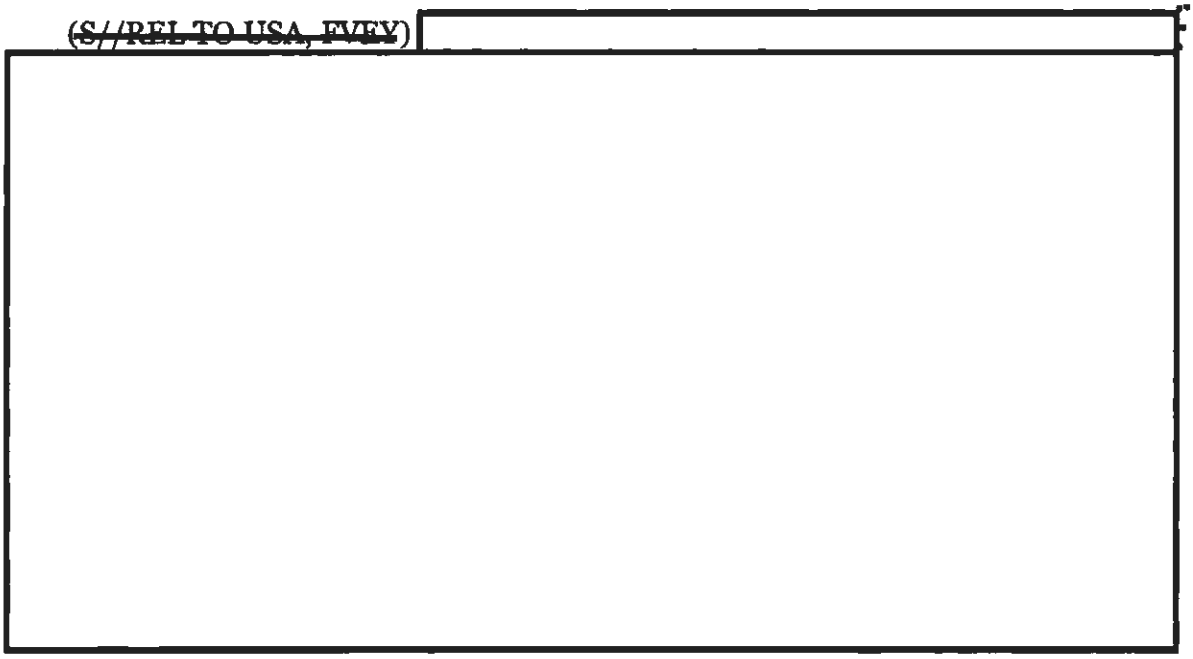
48 (U//~~FOUO~~)

49 (U//~~FOUO~~)

(~~TS//SI//REL TO USA, FVEY~~)

(~~TS//SI//REL TO USA, FVEY~~)

(~~S//REL TO USA, FVEY~~)



[50] (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

[51] (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

[52] (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]

~~(S//SI//REL TO USA, FVEY~~) Imagine you are researching the Constitutional Convention, so you go to the library to find books about James Madison's role. You know that there are many books about the Constitution and about James Madison; you only want books that concern both.

At the library, you consult the card catalog. It has one card for every book in the library. Each card lists certain attributes of its corresponding book: the date, the author, the publisher, its subjects. To find the books you want in this library, you search for cards that list both James Madison and the Constitution as subjects. When you find cards that fit those criteria, you read the corresponding books.

[redacted]

~~(S//SI//REL TO USA, FVEY)~~ [redacted]

[redacted]

~~(S//SI//REL TO USA, FVEY)~~ [redacted]

[redacted]

(b) (3)-P.L. 86-36

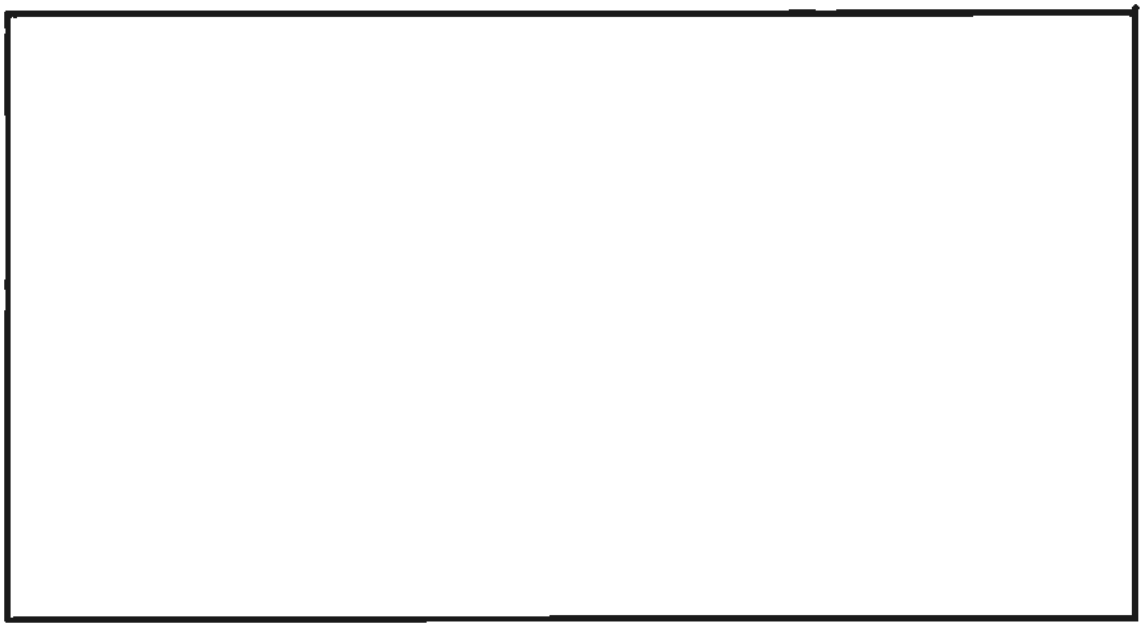
53 (U//~~FOUO~~) [redacted] handbook, p. 8 (2013).

54 (U//~~FOUO~~) NSA response to PCLOB draft, October 2020.

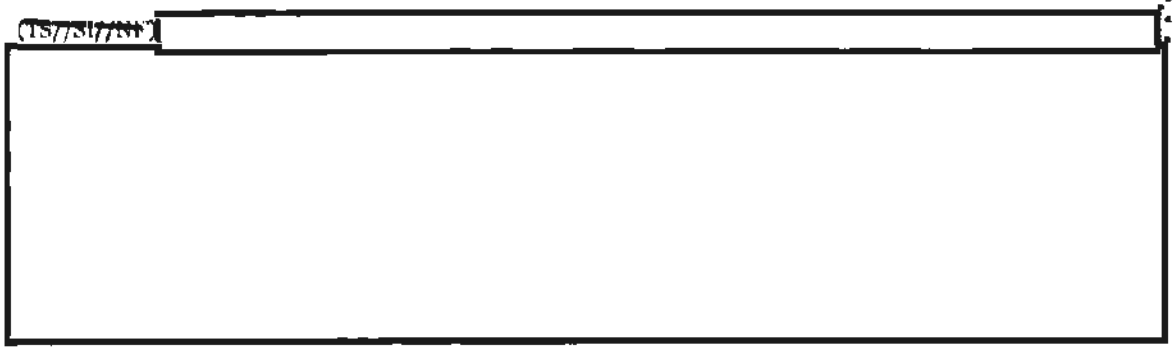
~~TOP SECRET//SI//NOFORN~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~



~~(TS//SI//NF)~~



~~(TS//SI//NF)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

3. ~~(U//FOUO)~~ XKEYSCORE as an Analytic Tool

~~(S//SI//REL TO USA, FVEY)~~ In using XKEYSCORE, analysts can run queries

~~(S//SI//REL TO USA, FVEY)~~

~~(S//SI//REL TO USA, FVEY)~~

~~(S//SI//REL TO USA, FVEY)~~

~~(S//SI//REL TO USA, FVEY)~~

~~(S//SI//REL TO USA, FVEY)~~ NSA analysts use XKEYSCORE

~~(TS//SI//NF)~~

(b) (3)-P.L. 86-36

[55] (U//~~FOUO~~) The decision to run queries in XKEYSCORE is a human one. While an analyst may set up queries to run multiple times, analysts decide what to look for,

[56] (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

[57] (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

[58] (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(~~S//REL TO USA, FVEY~~)

NSA analysts are trained to start with the narrowest and most tailored queries they can

(b) (3)-P.L. 86-36

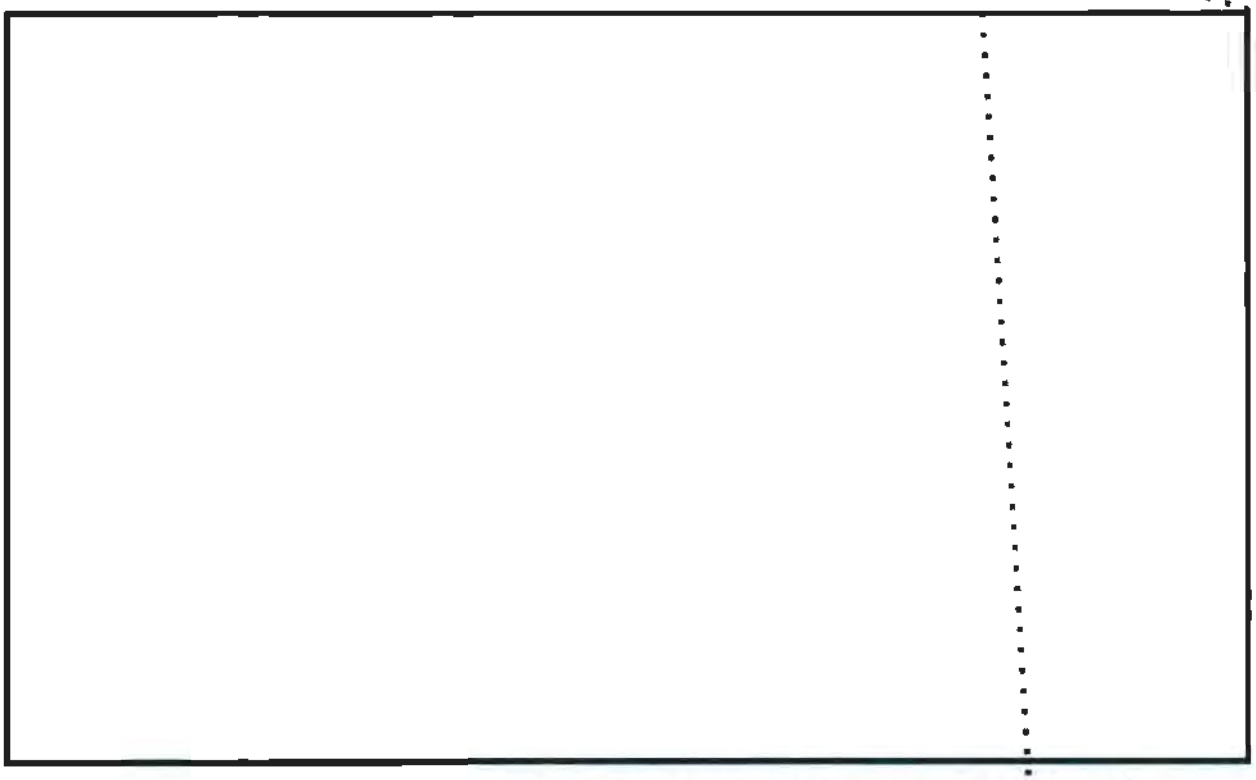
[59] (U//~~FOUO~~) NSA Answers to 2019 Tranche One PCLOB Questions (July 12, 2019).

[60] (U//~~FOUO~~)

[61] (U//~~FOUO~~) NSA Briefings and Demonstrations for the Board re: XKEYSCORE (Apr. 5, 2019).

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~



~~(S//SI//REL TO USA, FVEY)~~ The image above shows a portion of the query form an analyst would use when searching [redacted] The top of the image shows the basic information that must be filled in, including the name of the query and the justification for running it. The bottom part of the image shows where an analyst would set parameters for their query. In this image, the analyst would be creating a query [redacted]

(b) (3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(~~S//REL TO USA, FVEY~~)

(~~S//REL TO USA, FVEY~~)

(~~TS//SI//REL TO USA, FVEY~~)

(~~S//SI//REL TO USA, FVEY~~)

(~~TS//SI//REL TO USA, FVEY~~)

---

62 (~~S//REL TO USA, FVEY~~)

NSA Answers to 2019 Tranche One PCLOB Questions (July 12, 2019).

NSA response to notes from XKEYSCORE and survey and access briefings.

63 (~~S//REL TO USA, FVEY~~)

(b) (3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

C. (U) Operational Value

(~~S//SI//REL TO USA, FVEY~~) NSA analysts query XKEYSCORE primarily for target discovery and development.

(~~TS//SI//NF~~) NSA provided the Board with two historical examples that illustrate how XKEYSCORE has been used to advance the agency's counterterrorism mission.[67]

(b)(3)-P.L. 86-36

[64] (U//~~FOUO~~)

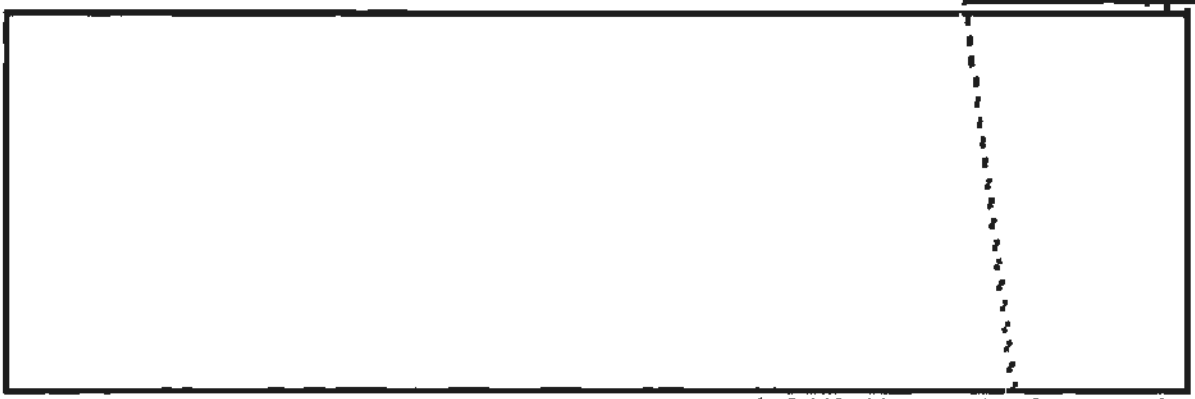
[65] (U//~~FOUO~~)

[66] (U//~~FOUO~~) NSA Briefings and Demonstrations for the Board re: XKEYSCORE (Apr. 5, 2019).

[67] (U//~~FOUO~~) NSA staff briefing to the Board on XKEYSCORE and Processing (July 23, 2015).

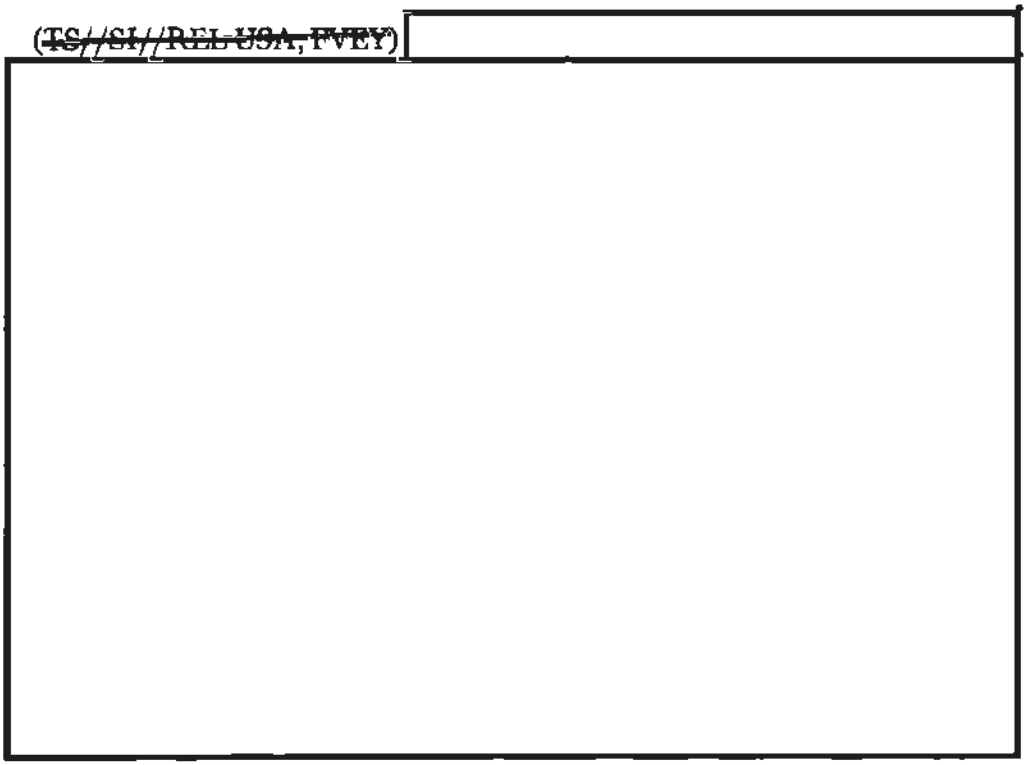
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~



~~(TS//SI//REL TO USA, FVEY)~~

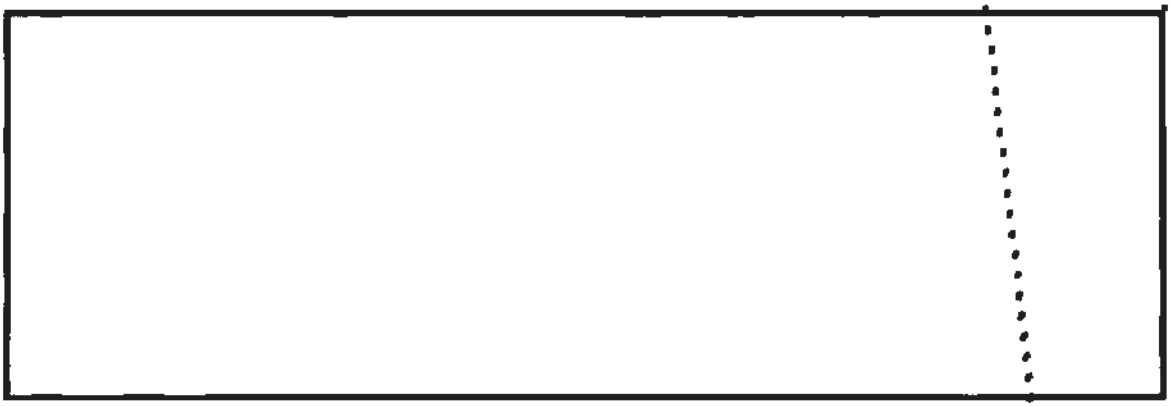
~~(TS//SI//REL TO USA, FVEY)~~



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

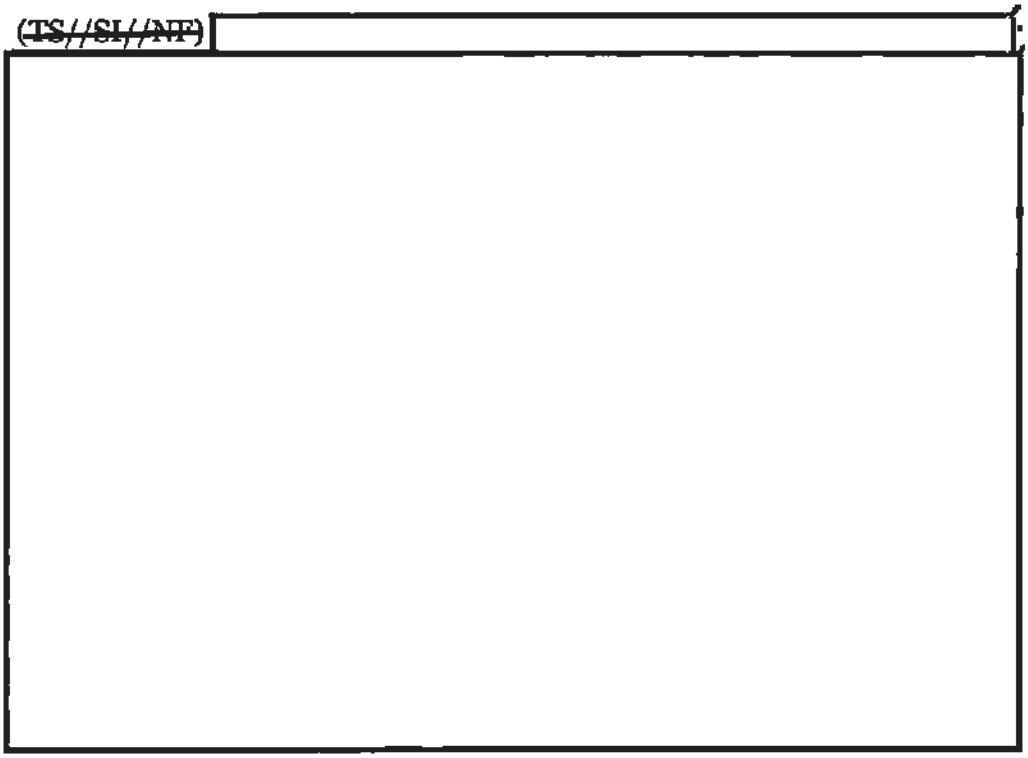
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY~~



~~(TS//SI//REL TO USA, FVEY)~~

~~(TS//SI//NF)~~



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

D. (U) Compliance Measures

1. (U) Auditing

(~~S//SI//REL TO USA, FVEY~~) NSA analysts' use of XKEYSCORE is subject to an extensive audit process. Notably, just as [redacted] is not part of XKEYSCORE, NSA's auditing capabilities are not part of XKEYSCORE. However, given how embedded the auditing process is within XKEYSCORE, it is difficult to understand one without the other.

(b)(3)-P.L. 86-36

(~~S//SI//REL TO USA, FVEY~~) Analysts must justify every query run in XKEYSCORE. The queries, along with those justifications, then go through NSA's auditing process, with NSA policy requiring that all queries be audited within [redacted] The core of this process are NSA employees who function as auditors. An auditor must be a US civilian or military NSA employee who (a) has completed all required compliance training and has the required access, (b) is working in the relevant SIGINT mission, and (c) is familiar with the targets and types of queries executed within the SIGINT mission by NSA personnel. To increase the efficacy of the reviews, auditors are required to understand the complexities of the queries that they review.[68]

(~~S//SI//REL TO USA, FVEY~~) To implement this auditing requirement, NSA relies on a tool called LEGALEAGLE. LEGALEAGLE allows auditors to see the queries run in their mission area, look at queries by specific users, or flag queries for additional review.[69] The auditors are reviewing the queries themselves for intent and compliance; they do not see the results of those queries.[70]

---

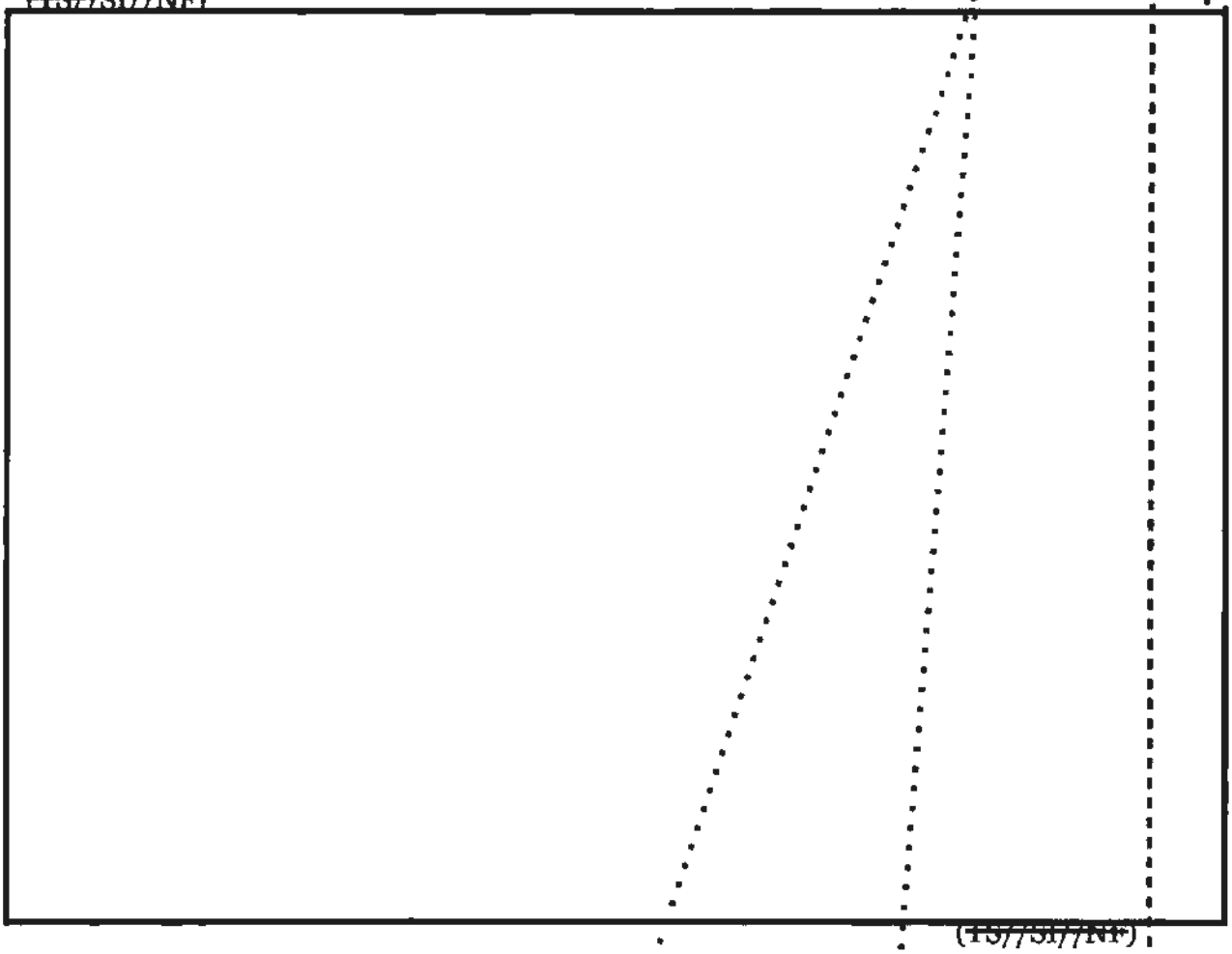
[68] (U) Phone call between NSA staff and PCLOB staff regarding NSA Deep Dive Follow-up Questions (Aug. 26, 2016).

[69] (U//~~FOUO~~) NSA Briefings and Demonstrations for the Board re: XKEYSCORE (Apr. 5, 2019).

[70] (U//~~FOUO~~) Notes from July 23, 2015 NSA Briefing on XKEYSCORE and Processing, with August 4 Follow-up Briefing at p. 28.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~



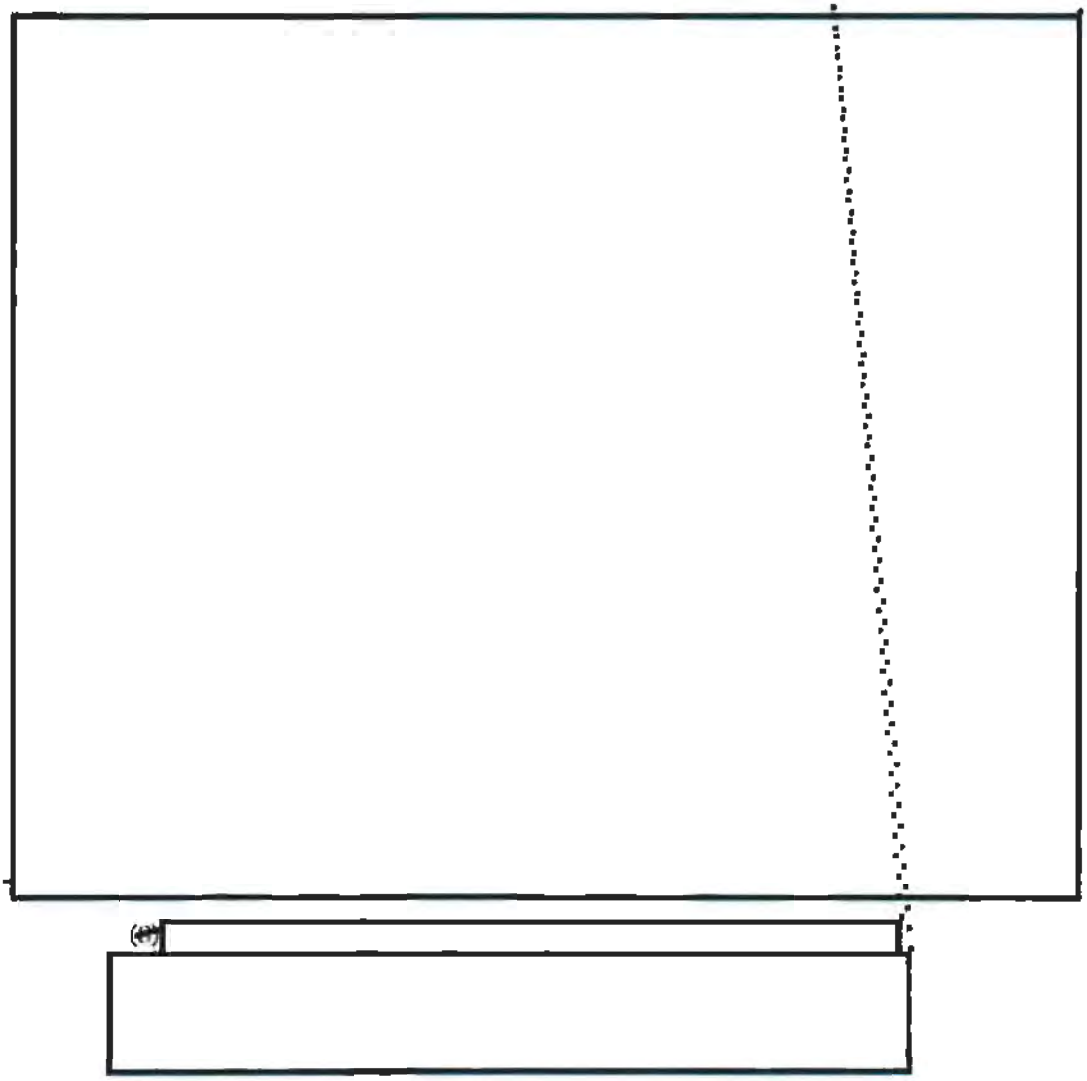
~~(TS//SI//NF)~~

~~(S//SI//REL TO USA, FVEY)~~ Not all XKEYSCORE queries carry the same compliance and privacy risks. For this reason, NSA has created systems to estimate the risk carried by each query. For example,

When auditors review queries, they are able to access key components of XKEYSCORE, directly from their auditing platform.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(~~TS//SI//NF~~)



(~~TS//SI//NF~~)

2. (U) Training and Access Limitations

(U//~~FOUO~~) NSA has oversight and compliance measures at nearly every stage of XKEYSCORE activity, from training to initial access to queries to an analyst's decision to disseminate a report. These measures are a combination of human review and automated systems designed to enforce compliance. NSA develops increasingly

complex technologies to enhance oversight and compliance measures, such as [redacted] to label queries as high- or low-risk.[71]

(U//~~FOUO~~) With respect to training, NSA requires that all personnel with the ability to review raw SIGINT data must complete online training and competency testing prior to accessing data in XKEYSCORE.[72] Mandatory training courses address topics such as USSID-18 provisions, the definition of USP information, intelligence oversight, SIGINT authorities, and legal requirements for SIGINT activities.[73] Some of these mandatory trainings are required for all NSA personnel, such as the NSA/CSS Intelligence Oversight Training; others, such as the NSA Raw Traffic Database Auditor Training, are limited to specific groups.[74]

(~~S//SI//REL TO USA, FVEY~~) There are also optional, XKEYSCORE-specific trainings.[75] While these trainings are not mandatory, NSA reports that they are completed by almost all new users of XKEYSCORE.[76] The trainings provide an overview of how XKEYSCORE works and how analysts can use it.[77] They also cover more advanced analytic applications, including [redacted] Trainings also reference compliance requirements.[78] For example, a training course instructs analysts to destroy USP communications as soon as feasible, and [redacted]

---

[71] (U//~~FOUO~~) NSA Briefings and Demonstrations for the Board re: XKEYSCORE (Apr. 5, 2019).

[72] (U) The mandatory trainings are not specific to XKEYSCORE.

[73] (U//~~FOUO~~) Trainings include: OVSC 1000 NSA/CSS Intelligence Oversight Training; OVSC 1100 Overview of Signals Intelligence (SIGINT) Authorities; OVSC 1800 USSID SP0018 Training for Analytic Personnel; OVSC 2201 SID Intelligence Oversight Officer Training; OVSC 3101 NSA Raw Traffic Database Auditor Training; PRIV1001 Annual Privacy Awareness Training; and PRIV1002 Privacy Training for Managers/Supervisors.

[74] (U) Notes from July 23, 2015 NSA Briefing on XKEYSCORE and Processing and August 4 Follow-up Briefing, at p. 17.

[75] (U//~~FOUO~~) [redacted]

[76] (U) Phone call between NSA staff and PCLOB staff regarding NSA Deep Dive Follow-up Questions (Aug. 26, 2016).

[77] (U//~~FOUO~~) [redacted]

[78] (U//~~FOUO~~) [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) NSA's training takes various forms. Certain traditional NSA training, such as those concerning NSA authorities under E.O. 12333, must be completed annually. NSA's required annual training is often text or video followed by a test that must be completed with a certain score. However, other NSA training is less traditional. For example, NSA has built a "gamification" system into XKEYSCORE's interface. Users gain "points" and "levels" by learning how to use progressively more advanced features of XKEYSCORE's analytic interface.

(U//~~FOUO~~) If an analyst has not completed the mandatory trainings, he or she will not receive the credential needed to access XKEYSCORE data—though completion of training is insufficient to gain access. An NSA system called [redacted] enforces training and other access limitations. Prior to accessing XKEYSCORE, NSA personnel must have completed mandatory training and be assigned to a mission in the [redacted] system. That is, the NSA analyst would need to have a job (which would have one or more "missions") that required access to XKEYSCORE data. Moreover, each authorized mission must have at least two auditors assigned to it. Any time a user attempts to access XKEYSCORE, [redacted] confirms there are still at least two valid auditors.[80]

(b)(3)-P.L. 86-36

ACCESSING XKEYSCORE

(U//~~FOUO~~) If an analyst works in the Operations Directorate and her duties require access to raw SIGINT data via XKEYSCORE, she must meet certain requirements to gain access—it's not enough to be an NSA employee. One of these requirements is an authorized mission: a focus area approved by the Director of the NSA via the Operations Director. For example, an authorized mission could be [redacted] NSA records authorized missions in [redacted] within [redacted]. In addition to describing the mission (here, [redacted]), [redacted] also lists the people who will perform certain roles (oversight, access sponsor, mission owner), provides the entitlements the mission requires (legal authorities, clearances, tools, data sources, etc.), and lists the members of the mission (the people who perform the jobs to accomplish the mission).

[79] (U) [redacted]

[80] (U//~~FOUO~~) NSA Briefings and Demonstrations for the Board re: XKEYSCORE (Apr. 5, 2019). For additional information on auditing, *see* Part III (D).

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

3. (U) Limitations on Data Use

(~~S//REL TO USA, FVEY~~) Part of what makes XKEYSCORE valuable is NSA's ability to parse and use the data. As explained at greater length above, NSA does extensive processing to enable users to access information they are looking for and [redacted] that could reveal targets or activities of foreign intelligence interest. This power comes with limitations though, primarily derived from the classified annex to Department of Defense Procedures Under Executive Order 12333 and United States Signals Intelligence Directive 18 "Legal Compliance and U.S. Persons Minimization Procedures" ("USSID-18"). NSA has explained that one of the most significant protections is that users are, generally speaking, unable to query on US persons. There are exceptions to this rule[81]—for example if someone consents or NSA has obtained approval from the Attorney General.[82] But NSA has explained that the volume of USP queries is exceedingly low—less than [redacted] in September 2019.

WHEN ARE USP QUERIES DONE?

- *(U) Consent*: NSA can conduct USP queries when it has consent, generally from their own employees or those of other government agencies who may be going into harm's way. NSA also uses consent as the basis to query for USP hostages, hoping they may find information leading to their rescue.
- *(U) Probable Cause*: NSA can conduct USP queries when it has obtained a probable cause order allowing electronic surveillance of a USP (typically an order from the FISA court).
- *(U) Attorney General Approval*: NSA can conduct USP queries when it has obtained Attorney General approval, which it sometimes does in addition to getting a probable cause order.

(~~S//REL TO USA, FVEY~~) Moreover, in running queries, analysts are required to provide a written justification of the intended foreign intelligence purpose for the query.[83] As discussed above, all of these justifications, as well as the underlying query terms, are audited.[84] These audits confirm that queries were properly tailored as well as consistent

[81] (U//~~FOUO~~) USSID SP0018, § 4.1(d).

[82] (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings. The ability for the Attorney General to approve these queries ultimately derives from E.O. 12333 §2.5. However, the Board understands that, since the passage of the FISA Amendments Act in 2008, NSA has obtained authorizations from the FISA court or pertinent emergency provisions within that statute. Thus, the Board is not aware of any subsequent instances where NSA has relied solely on the authorities in E.O. 12333 § 2.5.

[83] (U//~~FOUO~~) NSA response to notes from XKEYSCORE and survey and access briefings. *See* "Oversight and Compliance," Part III (D), for a discussion of the auditing process.

[84] (U) For more information on the approval and auditing process, *see* Part III (D).

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

with legal and policy limitations. For example, XKEYSCORE queries must be based on a foreign intelligence information need and must make attempts to limit US collection from the results.[85]

(~~S//REL TO USA, FVEY~~) NSA also points to back-end privacy protections that limit retention and dissemination of information obtained through XKEYSCORE. In order for an NSA analyst to use information found in XKEYSCORE, the analyst must [redacted] – a human choice that does not happen automatically. When making such a determination, NSA analysts provide a foreign intelligence justification [redacted][86] Moreover, when information [redacted] the Attorney General Guidelines and NSA policies govern its handling. Pertinent here is Section 309 of the Intelligence Authorization Act of 2015 and USSID-18 § 6, governing the retention of communications to, from, or about US persons. XKEYSCORE-obtained information [redacted] must still comport with the access restrictions as well as limits on retention found in that section.[87]

(~~S//SI//REL TO USA, FVEY~~) Under USSID-18, [redacted] that data can be stored for five years, although in practice it may be shorter due to storage space limitations. This data is tagged and regularly, automatically checked to ensure that it is deleted from NSA repositories if it is the subject of a compliance issue or retention limits. XKEYSCORE data can only be stored indefinitely when an analyst has evaluated and minimized it, or when NSA reporting relies on the data.

(~~S//REL TO USA, FVEY~~) When USP information is used in an intelligence report, there are further restrictions. Pursuant to NSA's minimization procedures, NSA may not disseminate non-publicly available information of or concerning a US person

(b) (3)-P.L. 86-36

[85] (U//~~FOUO~~) NSA policy also requires analysts to limit collection associated with [redacted]

[redacted] (~~S//REL TO USA, FVEY~~)

(~~S//SI//REL TO USA, FVEY~~) Some caveats apply here. NSA analysts were required to provide a foreign intelligence justification [redacted] because a legacy system required it to function, not because of a legal or policy requirement. While analysts provide a foreign intelligence justification, it is not checked by auditors and is only done for the benefit of the analyst. NSA Briefing on XKEYSCORE (Feb. 7, 2019 and July 23, 2020).

[87] (U//~~FOUO~~) NSA Answers to 2019 Tranche One PCLOB Questions (July 12, 2019).

absent that person's consent, unless a determination is made that such information is necessary to understand or access foreign intelligence. Even then, as a matter of policy, NSA generally does not include the names of US persons in their intelligence reports. Instead, they "mask" the names, using a generic term such as "US person 1."[88] This is because often only a subset of the recipients of the intelligence report need to know the USP information to perform their duties. NSA also provides its analysts with comprehensive guidance on how to properly reference masked US person identities in reporting. This guidance emphasizes the need to avoid contextual identification, which occurs if the identity of a US person is masked, but there are enough other pertinent details that a recipient can identify the US person anyway.

Masking and unmasking

(U) Generally speaking, pursuant to NSA's minimization procedures, a US person identity may be disseminated only if it is necessary to understand or assess the foreign intelligence. Even then, NSA will "mask" the identity in the report by replacing a name or other unique identifier with text like "US Person 1."

(U) If an identity has been masked, but an authorized recipient of the report feels that they need the information to carry out their duties, they can request NSA to unmask the identity. If that request is approved by the NSA director or a designee, the other entity would be provided with the unmasked US person identity.

~~(S//REL TO USA, FVEY~~) If another agency then wants to know the identity of the US person, that requires written documentation and approval. Among other things, NSA requires "a fact-based justification" of why each individual who will receive the US person identity needs it to carry out their duties.[89] This request for "unmasking" can only be approved by the NSA Director or a designee.[90]

~~(S//SI//REL TO USA, FVEY~~) In limited circumstances, NSA analysts may proactively identify a US person by name, title, or context in a report. For instance, NSA policy permits identifying certain senior US officials by title in a report. Additionally, there may be a "blanket dissemination authority" for a US person

[88] (U) *See generally*, NSA Policy 2-4, *Handling of Requests for Release of US Identities*, May 10, 2019.

[89] (U) NATIONAL SECURITY AGENCY, HANDLING OF REQUESTS FOR RELEASE OF U.S. IDENTITIES, NSA/CSS Policy 2-4 (May 10, 2019). NSA policy allows for oral requests in exigent circumstances. However, the requesting entity must provide their basis using the traditional process within five days of the identity being disclosed.

[90] (U) NATIONAL SECURITY AGENCY, HANDLING OF REQUESTS FOR RELEASE OF U.S. IDENTITIES, NSA/CSS Policy 2-4 (May 10, 2019).

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

identity where the appropriate officials have determined that the identity is necessary to understand or assess the foreign intelligence on a recurring basis, and that all recipients of the reporting will require that information to perform their official duties. This may be the case, for example, if [redacted] happens to be a US person as well (and therefore the subject of a Section 704 order issued by the FISA court). Any unmasking of USP information is strictly controlled, however, and NSA's [redacted] group reviews each instance.

4. (U) Oversight

(U//~~FOUO~~) As a general rule, these compliance and oversight measures, including training requirements, handling of data, and auditing, fall to NSA's Compliance Group. The Compliance Group is responsible for routine oversight and compliance matters and supporting NSA's Intelligence Oversight Officer in implementing SIGINT compliance programs.[91] The Compliance Group also engages in higher-level oversight, such as "super audits"[92] where they audit the auditors, and "compliance verification."[93]

~~(U//FOUO)~~ The Compliance Group conducts site assistance visits, where they examine the compliance measures in place.[94] They assess procedures against existing standards, confirm that safeguards are operating as intended, and recommend improvements.[95] When doing super audits, the Compliance Group review query terms run in XKEYSCORE. [redacted] super audits do not look at the results of an XKEYSCORE query—only the query itself. Finally, compliance verification includes testing of purge procedures.[96]

(U//~~FOUO~~) The Compliance Group is not the only entity ensuring compliance with law and policy. Depending on the issue, the Office of General Counsel or the Inspector

(b) (3)-P.L. 86-36

[91] (U) USSID-19 § 4.7.

[92] (U) Super auditing is the independent review of activities conducted against raw SIGINT systems, tools, or databases. USSID-19 § 5.

[93] (U) USSID-19 § 4.7.

[94] (U) USSID-19 § 4.7.

[95] (U) USSID-19 § 4.7.

[96] (U) USSID-19 § 4.7.

General may also get involved. NSA has explained that "[o]n occasion, decisions about particular collections will require a risk assessment and/or additional specific feedback relating legal and policy considerations."[97] In such instances, the Office of General Counsel, as well as the Civil Liberties Privacy and Transparency Office and the Risk Management Office, would be consulted.[98]

[redacted] ~~(U//FOUO)~~ However, when asked, NSA did not provide any examples from the many years of XKEYSCORE's operation in which the Office of General Counsel or the Civil Liberties, Privacy and Transparency Office provided legal, policy, or risk assessments on particular decisions. NSA declined to provide examples where either office consulted on the selection [redacted] Further, neither office has ever provided overarching guidance on the legal, privacy, or risk considerations that NSA technical personnel should use when [redacted]

[97] (U) NSA Answers to PCLOB Questions (Aug. 6, 2019).

[98] (U) NSA Answers to PCLOB Questions (Aug. 6, 2019).

IV. (U) NSA's Analysis of XKEYSCORE

A. (U) Background on E.O. 12333

(U) The specific authority NSA cites for its XKEYSCORE activities is Executive Order 12333. Section 1.7(c) of that order sets out general duties and responsibilities of NSA, while Section 2 discusses how NSA should conduct its intelligence activities. Within the order, Sections 2.3 and 2.4 are the most pertinent to the protection of USPs in the course of the covered activities. Section 2.3 regards the collection, retention, and dissemination of USP information. Section 2.4 discusses collection techniques and requires agencies to have specialized procedures regarding their use of particular techniques.[99]

(U) The requirement for specialized procedures leads to the most detailed authorities for NSA activities: Attorney General-approved guidelines for engaging in specified intelligence activities. As a component within the Department of Defense (DoD), NSA is subject to the DoD's Attorney General-approved procedures, DoD Manual (DoDM) 5240.01. NSA is also governed by the classified annex to DoDM5240.1 as well as certain supplemental procedures that are not applicable to XKEYSCORE. These policies each implement E.O. 12333 at various levels of granularity. DoDM 5240.01 is the Attorney General-approved DoD procedure for the collection, retention, and dissemination of information concerning USPs as well as the use of various intelligence techniques. While NSA is bound by this, the classified annex to 5240.1-R contains the Attorney General-approved procedures specifically for the collection of SIGINT, and thus provides more detail on NSA-specific SIGINT activities.

(U//~~FOUO~~) In addition to the Attorney General-approved procedures, NSA has created internal policies and implementing documents. The foremost is United States Signals Intelligence Directive No. SP0018, "Legal Compliance and U.S. Persons Minimization Procedures" ("USSID-18"). Naturally, implementing guidance such as USSID-18 is more specific than the Attorney General guidelines in defining permissible and impermissible activities. Thus, for NSA, questions about the permissibility of SIGINT activities do not start with E.O 12333 but with USSID-18, the classified annex to 5240.1-R, and then DoDM 5240.01. These documents implement

---

[99] (U) E.O. 12333.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

Sections 2.3 and 2.4 of E.O. 12333, but do so in a way that accounts for the specific intelligence activities being undertaken.[100]

~~(S//REL TO USA, FVEY)~~

B. ~~(S)~~ NSA Explanation Regarding [redacted] and Selection

(U//~~FOUO~~) NSA locates its authority to run XKEYSCORE in E.O. 12333's mandate that NSA "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes." This authority, they explain, allows them not only to collect known foreign intelligence signals, but also to engage in "search and development" operations, where NSA looks for signals containing foreign intelligence, though they know that in the process they may collect information that is not itself foreign intelligence information. This is most clearly articulated in USSID-18, annex E, "Search and Development Operations." However, it is rooted in E.O. 12333 and the classified annex to DoD's Attorney General guidelines.

(~~S//REL TO USA, FVEY~~) XKEYSCORE collects foreign intelligence as defined in E.O. 12333. There, foreign intelligence is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists."[101] The "activities of . . . foreign persons" is broad—there is no requirement that the foreign person be a terrorist or spy, nor that the activity be illegal or undertaken on behalf of a foreign power. However, it is not unlimited. In addition to limitations on USP collection built into E.O. 12333, the classified annex explains that "it is the policy of the United States Signals Intelligence System to collect, retain, and disseminate only foreign communications and military tactical communications."[102] Moreover, it limits the collection of USP communications by noting that such communications "may be

[100] (U//~~FOUO~~) On August 8, 2016, the Attorney General-approved DoDM 5240.01: Procedures Governing the Conduct of DoD Intelligence Activities and cancelled procedures 1-10 of DoD 5240.1-R: Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons. For much of the time period covered by the Board's review, the earlier DoD procedures were in effect. The classified annex to DoDM 5240.01-R remains in effect. After review, NSA determined that 5240.01 did not impact the operation of XKEYSCORE. NSA Answers to PCLOB Questions, Aug. 6, 2019.

[101] (U) E.O. 12333 § 3.5(e).

[102] (U) DoD Regulation 5240.1-R Classified Annex § 3.

intercepted intentionally" only in certain circumstances, such as with the consent of the USP or pursuant to a court order.[103]

(~~C//REL TO USA, FVEY~~) The National Intelligence Priorities Framework (NIPF) contains foreign intelligence priorities that guide the IC's collection and analytic activities.[104] This framework is then translated into requirements for the various elements of the intelligence community. NSA's specific SIGINT collection requirements come from the National Signals Intelligence Committee, the group that is responsible for translating the NIPF priorities into signals intelligence "information needs." [redacted] are based on an assessment of what is most likely to obtain foreign intelligence information responsive to the identified information needs.

(~~S//REL TO USA, FVEY~~) Within this effort to gather information based on legitimate information needs, NSA must also "make[] every reasonable effort, through surveys and technical means, to reduce to the maximum extent possible the number of [USP] incidental intercepts acquired in the conduct of its operations."[105] [redacted]

[redacted]

[103] (U) DoD Regulation 5240.1-R Classified Annex § 4(1).

[104] (U) Intelligence Community Directive (ICD) 204: National Intelligence Priorities Framework § D1 (Jan. 2, 2015).

[105] (U) DoD Regulation 5240.1-R Classified Annex § 3.

[106] (U) Phone call between NSA staff and PCLOB staff regarding NSA Deep Dive Follow-up Questions (Aug. 26, 2016).

[107] (U) NSA noted that the 2011 Judge Bates opinion describes exceptions to this presumption. Phone call between NSA staff and PCLOB staff regarding NSA Deep Dive Follow-up Questions (Aug. 26, 2016).

[redacted] (~~S//REL TO USA, FVEY~~) (U//FOUO) [redacted] Phone call between NSA staff and PCLOB staff regarding NSA Deep Dive Follow-up Questions (Aug. 26, 2016).

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//REL TO USA, FVEY)~~

NSA must therefore make educated guesses about whether it will obtain mostly foreign information and whether it will likely obtain information of interest [109]

~~(S//REL TO USA, FVEY)~~

~~(S//REL TO USA, FVEY)~~ NSA asserts that its appropriately balance the imperative to collect foreign intelligence information with the limits on collection of USP information by excluding communications and by focusing its efforts on predefined intelligence priorities. In those instances where USP communications are acquired, NSA asserts that the collection is incidental and remains reasonable under the totality of the circumstances given the back-end restrictions on the use of USP communications.

[109] (~~U//FOUO~~) NSA Briefing on XKEYSCORE (Feb. 7, 2019). As noted above, because US person information is unlikely to contain the foreign intelligence NSA seeks,

[110] (U) *Cf.* Classified Annex §4 (limiting the *intentional* acquisition of USP communications) and USSID-18 Annex E (explaining how to handle USP information obtained as part of a search and development operation).

V. (U) PCLOB Recommendations

A. (U) Recommendations from the Board

~~(TS//SI//REL TO USA, FVEY)~~ XKEYSCORE raises important and complex questions of law and policy. These questions arise in a rapidly changing technological and legal environment and against a backdrop of a program that continues to evolve. The Board offers the following recommendations to help NSA and other entities implement and oversee XKEYSCORE.

(U) Recommendation 1: NSA should conduct and periodically review and update a legal analysis of XKEYSCORE.

~~(S//SI//REL TO USA, FVEY)~~ NSA's existing legal analysis of XKEYSCORE elides certain difficult questions. On its own or with the Department of Justice, NSA should conduct a rigorous legal analysis of XKEYSCORE and periodically update that analysis as law and technology change. Specifically, the Board recommends that the agency consider the following, non-exhaustive list of constitutional questions in analyzing the program.

Fourth Amendment

- Which actions by the government are "searches" or "seizures" within the meaning of the Fourth Amendment?
- Where do those searches or seizures take place, specifically, do they take place within the United States, at the border, or outside? How does the location affect the constitutional analysis?
- Does the Amendment's warrant clause apply, or must the government's action meet only the "reasonableness" standard?
- If the warrant requirement applies to a specific search or seizure, is there an applicable exception (for example, the foreign intelligence exception)?
- To the extent a reasonableness inquiry is applicable, what are the relevant privacy interests and agency interests? Do these interests vary based on the location of the search or seizure, and if so, how?

First Amendment

- Consider whether the First Amendment is applicable.

~~(S//SI//REL TO USA, FVEY)~~ In addition to these constitutional questions, NSA should consider XKEYSCORE's compliance with applicable statutes, Executive Order

12333, DOD Manual 5240.01, and other applicable legal instruments. Its analysis should reflect the fact [redacted] Moreover, its analysis should be periodically reviewed and updated to account for technological, legal, and mission-related changes.

(U) Recommendation 2: The Classified Annex to Department of Defense Manual 5240.01 and NSA's implementing guidance should be updated to reflect changes to the manual.

(U//~~FOUO~~) Attorney General-approved guidelines under Executive Order 12333 help ensure that the nation's intelligence collection efforts safeguard privacy and civil liberties of US persons. And yet, when the Board began its Executive Order 12333 investigation, many guidelines, including those of the Department of Defense, had not been updated since the 1980s.

(U//~~FOUO~~) Since then, there have been several updates. The Department of Defense updated its Attorney General-approved guidelines under Executive Order 12333 in 2016.[111]

(~~TS//SI//NF~~) At the time of this report's publication, NSA, the Department of Defense, and the Department of Justice are in the final stages of updating the Classified Annex.[112] The Board recommends that, as NSA continues to update the annex, NSA develop robust guidance for issues, such as [redacted] that undergird XKEYSCORE's distinctly modern search-and-discovery capabilities.

(U//~~FOUO~~) USSID-18 should also be updated to ensure consistency with the current Attorney General-approved guidelines and approved operational practices. For example, the definition of "collection" in USSID-18 should be consistent with the definition found within Department of Defense's current Attorney General-approved guidelines. Changes to requirements for search-and-discovery activities in the Classified Annex should also be reflected in implementing guidance.

[111] See Department of Defense Manual 5240.01.

[112] The Board gave some input on this draft of the Annex; Board Member Elisebeth Collins advised on the draft in 2018, while the Board was inquorate, and the full Board was briefed on the Annex in the fall of 2020.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) Recommendation 3: NSA should notify the Board of changes to XKEYSCORE that could materially affect the privacy or civil liberties of US persons.

(~~S//NF~~) Technological, operational, or policy changes could significantly alter XKEYSCORE's degree of intrusiveness for US persons. For example, [redacted] could materially shift the balance between operational equities and privacy protection. As XKEYSCORE evolves, NSA should notify the Board of changes in technology, operations, or policy that could materially affect the privacy or civil liberties of US persons.

(~~U~~) Recommendation 4: NSA should engage its Office of General Counsel and Civil Liberties Privacy and Transparency Office in [redacted] decisions.

(~~S//NF~~) NSA has explained that "[o]n occasion, decisions about [redacted] will require a risk assessment and/or additional specific feedback relating legal and policy considerations." In theory, NSA would consult its Office of General Counsel (OGC) and Civil Liberties Privacy and Transparency Office (CLPT) in such instances. However, NSA did not provide any real-world examples in which OGC or CLPT provided legal, policy, or risk assessments on particular [redacted] decisions. Nor has either office provided overarching guidance or legal advice regarding the legal, privacy, or risk considerations that should be evaluated by NSA technical personnel during the process of [redacted] for collection.

(~~TS//SI//NF~~) NSA operational personnel should engage these two offices to consider the legal and privacy implications of [redacted] decisions. Specifically, as [redacted] operational personnel should consult with these offices in establishing the rules by which automated systems will [redacted].

(~~S//NF~~) Recommendation 5: NSA should include XKEYSCORE-specific content in the training required before analysts can use XKEYSCORE.

(~~S//SI//REL TO USA, FVEY~~) Currently, NSA requires analysts to complete some trainings before they can use XKEYSCORE. These trainings are not XKEYSCORE-specific, however, and concern SIGINT more generally. Because XKEYSCORE's search-and-discovery capabilities distinguish it from other SIGINT tools, the Board

recommends that NSA include XKEYSCORE-specific content in the training that analysts are required to complete before beginning to use XKEYSCORE.

(U) Recommendation 6: The Office of the Director of National Intelligence and NSA should share best practices and (where possible) technical solutions from NSA's auditing architecture with other IC agencies that hold comparably sensitive large datasets.

~~(S//SI//REL TO USA, FVEY)~~ The Office of the Director of National Intelligence should work with NSA to share best practices from NSA's auditing architecture with other IC agencies that maintain large datasets that are likely to contain potentially sensitive information about Americans. ODNI and NSA should also assess whether technical elements of NSA's audit system can be adopted by other agencies, consistent with the protection of classified methods. Other agencies appear to be far behind NSA in the fitness-for-purpose of their audit systems. The assistance envisioned here would help close the gap.

(U) Recommendation 7: NSA should periodically provide the Board with information about the number and nature of XKEYSCORE queries resulting in significant compliance findings, including any pertaining to U.S. persons.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

B. (U) Additional Recommendations from Board Members Edward Felten and Travis LeBlanc

(~~TS//SI//NF~~) NSA should study

(~~TS//SI//NF~~)

(~~TS//SI//NF~~)

(~~S//NF~~) XKEYSCORE analysts should be required to tag or take other reasonable measures to identify known or believed U.S. person data

(~~U//FOUO~~) In other words, if the analyst knows or believes contains USP information, they should so tag it.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~(S//SI//REL)~~ NSA should affirmatively deprioritize U.S. person data processed by XKEYSCORE.

~~(S//REL TO USA, FVEY)~~ We understand that NSA seeks to prioritize its XKEYSCORE collection and analysis efforts on information [redacted] that are likely to have foreign intelligence value. This prioritization system is designed to prioritize the collection of foreign intelligence over, what NSA calls, "superfluous" traffic, [redacted] NSA asserts that by prioritizing foreign intelligence it *de facto* deprioritizes the collection of "superfluous" data such as that involving U.S. persons. We believe that the prioritization of foreign intelligence alone is not sufficient to properly guard against the collection and processing of U.S. person data, which is protected by law and the Constitution. We therefore recommend that NSA affirmatively deprioritize U.S. person data [redacted]

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

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

Additional views of Chairman Adam Klein

(U) I join in full our report on XKEYSCORE and am grateful to the staff members whose diligence and expertise enabled us to successfully conclude this long-running project. I write separately to offer additional thoughts on XKEYSCORE's value and accompanying privacy safeguards.

(~~S//REL~~) First things first: There should be little doubt that XKEYSCORE is highly effective at discovering foreign intelligence that can be used to protect the United States.

(~~S//SI//REL~~)

(~~TS//SI//NF~~) NSA has provided several vignettes demonstrating XKEYSCORE's contribution to specific counterterrorism successes.

(U) Powerful tools like XKEYSCORE must be constrained by law and policy, and these laws and policies must be enforced by effective compliance and oversight mechanisms. XKEYSCORE operates within well-established legal and policy constraints, which are enforced by the compliance infrastructure at NSA.

(~~S//SI//REL~~) Some of these constraints limit the information that comes into XKEYSCORE and how long it remains there:

- (U) Title VII of the Foreign Intelligence Surveillance Act prohibits the use of NSA's EO 12333 SIGINT infrastructure, including XKEYSCORE, to target U.S. persons for collection of content without probable cause, consent, or an emergency authorization from the Attorney General.[1]
- (~~TS//SI//REL~~)

(~~S//SI//REL~~) Other safeguards regulate how the information can be accessed and used That is important. In the digital era, effective intelligence is, to a significant degree, an exercise in collecting and analyzing large datasets. By virtue of the volume of traffic and the interconnected, borderless nature of modern telecommunications, collection on this scale will inevitably include information about Americans. Once information about Americans comes into an agency's

[1] *See* 50 U.S.C. § 1881c.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

hands, it is the task of law, policy, technical controls, institutional safeguards, and agency culture to limit its use. The wider the aperture for front-end collection, the more important these back-end protections become.

(~~S//SI//REL~~) XKEYSCORE has a wide aperture, so it is appropriate that it includes significant back-end protections. Most notably:

- (~~S//REL~~) Analysts are prohibited from running U.S.-person queries in XKEYSCORE, subject to very narrow exceptions. Analysts can run U.S.-person queries only with a probable-cause order from the FISA Court, consent, or approval from the Attorney General.[2]
- (~~S//REL~~) All XKEYSCORE queries are subject to robust, technologically advanced logging and auditing, which our report describes in detail. As part of this system:
  - (~~S//REL~~) Analysts must provide detailed, non-formulaic justifications for each query.
  - (~~S//REL~~) Each query is logged; these logs include the analyst's justification and various other telltale details about the query.
  - (~~S//SI//REL~~) NSA's auditing system uses [redacted]s to help identify queries that may be insufficiently tailored or non-compliant. Human auditors familiar with the analyst's mission then review every query deemed to pose a risk of noncompliance.
  - (~~S//SI//REL~~) Under NSA rules, queries based on broad criteria must be tailored to avoid returning information that is not foreign intelligence.[3]
- (~~S//REL~~) If an analyst's query returns information about an American, NSA policies limit how that information can be used, retained, and disseminated.[4]

(~~S//SI//REL~~) The auditing architecture, described in Part III.D.1 of our report, is noteworthy. The system enables meaningful scrutiny, in close to real time, and appears to be much more effective and comprehensive than the post hoc site visits and manual spot checks on which some other agencies rely.

(~~S//NF~~) Our Board reviews large-scale collection programs across IC and non-IC agencies. It is noteworthy that while NSA has developed sophisticated technical capabilities to log queries, to record query justifications, [redacted] and to organize queries for efficient review by human auditors, systems in use at other agencies are less advanced. As Recommendation 6 from the Board's report envisions, NSA's audit

[2] (U) *See* Parts III.D.3 and IV.A.

[3] (~~S//SI//REL~~) *See* USSID-18 § 5.1(c) ([redacted] "SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.").

[1] *See, e.g.*, DoDM 5240.1 and Classified Annex: USSID-18.

program can offer a useful example (and perhaps some technical solutions) to other IC elements seeking to ensure effective oversight of their personnel's access to large, sensitive datasets.

(U) Of course, the adequacy of the controls we have identified depends on how effectively and thoroughly they are implemented, and on vigorous monitoring. The Board will monitor the implementation of the recommendations in this report and remain alert to significant changes in how XKEYSCORE is deployed going forward.

(U) Separate Statement of Board Member Ed Felten

(U) I concur in the Board's report, and join my colleagues in thanking the Board's staff for their careful, skilled, and diligent work on this report. I will comment briefly on two topics.

1. Policy Implications of XKEYSCORE

(U) XKEYSCORE raises policy issues that are likely to grow in importance as technology advances and NSA's capabilities continue to develop. This makes it especially important for NSA to develop a clear legal and policy rationale for XKEYSCORE. Such an analysis will not only guide the agency's development of XKEYSCORE, but will also establish a framework useful for evaluating future programs.

~~(TS//SI//REL)~~ It is useful to consider separately two primary policy-relevant capabilities of XKEYSCORE: [redacted]

~~(TS//SI//REL)~~ [redacted] are valuable foreign intelligence capabilities, assuming they are applied to data that is appropriately collected and managed. I applaud NSA's work to advance these capabilities.

~~(TS//SI//REL)~~ Data retention is a more challenging policy issue. XKEYSCORE's ability to "collect SIGINT [redacted] has obvious mission value. However, [redacted], some of it inevitably including U.S. person communications, must be justified in light of our national values and relevant law including the Fourth Amendment.

~~(TS//SI//REL)~~ At present, practical factors of storage and cost limit NSA's retention of data and thereby serve as a limit on the intrusiveness of this capability. But that could easily change as technology advances, if storage and analysis capacity increase faster than the volume of targeted communications traffic. Indeed, that seems likely to be the case for more and more categories of communications. Accordingly, it is important for NSA to consider carefully where to draw the line on data retention, and especially on the principles underlying that policy and legal determination. It must be clear where to draw the line on retention.

(U//~~FOUO~~) Though NSA should apply its technical, mission, and legal expertise to questions of data retention, the question of where to draw the line on data retention is important enough to merit attention from Congress and national leadership.

2. Deprioritization of U.S. Person Data

~~(S//SI//REL)~~ NSA appropriately prioritizes collection of foreign intelligence. As a result, it collects less information that is superfluous, that is, not foreign intelligence. My

colleague Travis LeBlanc and I recommend that NSA additionally take affirmative steps to deprioritize U.S. person information.

~~(S//SI//REL)~~ For discussion purposes, one might divide the information available for collection and analysis into three categories: foreign intelligence (FI), U.S. person information (USPI), and everything else (Other). NSA wants to collect and analyze FI and does not want to collect or analyze USP or Other information. For information that falls clearly into one category or another, NSA knows what to do and has systems in place to ensure compliance.

~~(S//SI//REL)~~ But much information cannot be categorized so clearly, [redacted] Here NSA does what it can, based on the information available. This is inherently a balancing decision process based on the likelihood of the information being in each category.

~~(S//SI//REL)~~ Our recommendation calls on NSA to include in this decision process not only the likelihood that information is FI, but also the likelihood that it is USP information versus Other information. In other words, if information is two percent likely to be FI, it should matter whether the other ninety-eight percent of likelihood falls into the USP category or the Other category.

~~(S//SI//REL)~~ Reasonable people can disagree about how much weight to place on the goal of collecting and using FI versus the goal of avoiding incidental or non-targeted collection and use of USPI. But surely the answer cannot be that the presence of USPI has no bearing at all on whether collection is lawful and wise. Surely the presence of the smallest iota of FI, in an ocean of USPI, cannot be dispositive.

~~(TS//SI//REL)~~ [redacted] but NSA should in any case have technical and administrative measures in place to deprioritize USPI relative to superfluous foreign information, as well as a careful legal and policy rationale supporting those measures.

(U) Statement of Board Member Janie Nitze

(U//~~FOUO~~) I am pleased to join in full the Board's report on XKEYSCORE, and, like my colleagues, offer my gratitude to the staff members whose hard work enabled us to bring the project to completion.

(~~S//REL~~) I also join the Chairman's separate statement, which reviews the utility of XKEYSCORE and the important back-end safeguards that allow the tool to operate within well-established legal and policy constraints. I write separately to note my concerns with two of the minority recommendations.

(~~TS//SI//NF~~) *Minority Recommendation 2.* The full text of minority recommendation 2 reads:

> XKEYSCORE analysts should be required to tag or take other reasonable measures to identify known or believed U.S. person data [redacted]. In other words, if the analyst knows or believes that datel [redacted] contains USP data, they should so tag it [redacted]

(U) Respectfully, I decline to join the recommendation for the following reasons.

(~~TS//SI//NF~~) As an initial matter, the recommendation does not use terms defined and routinely used by the intelligence community, but instead refers to "known or believed U.S. person data." That leaves the breath of the recommendation uncertain. Does the term "U.S. person data" cover only information where a U.S. person is a communicant? Or does it also include information about U.S. persons? Or does it go so far as to refer to data *created* by U.S. persons, which a plain reading of the term "U.S. person data" would suggest?

(~~TS//SI//NF~~) Although each potential meaning of the term changes the recommendation's operational impact, a few general observations can be made. *First*, requiring analysts to "tag or take reasonable measures to identify known or believed U.S. person data" injects uncertainty [redacted] After all, what is an analyst to do if he is *pretty sure*, but not certain, that information is "U.S. person data"? Is he to tag the information regardless of his uncertainty (thereby introducing potential errors into the dataset)? Or is he to ignore the tagging requirement unless he's sure (which may not often be the case)? Or is the analyst to research the question, perhaps poke around various datasets and see what he can find about the communicant or information in question? Of course such research would seemingly be to the detriment of U.S. person privacy, as it could well entail analysts learning *more* about a U.S. person or his information than in the absence of the tagging requirement. Moreover, some research surely would be barred by policy and legal documents that seek to protect USPI – introducing a compliance trap and yet more confusion into what an analyst is to do.

(~~TS//SI//NF~~) *Second*, the point of the tagging requirement is unclear. Analysts are already required to follow various procedures set in place to protect U.S. person privacy. For example, the DoDM requires analysts to "[t]ailor queries or other techniques to the greatest extent practicable to minimize the amount of USPI returned that is not pertinent to the intelligence mission and purpose for the query."[1] Consider the case of an analyst that runs a query that returns information containing valuable foreign intelligence now tagged as "U.S. person data." To the extent the analyst could access that information as before, the new tagging requirement creates no new restriction on the use, analysis, or dissemination of USPI. To the extent, though, my colleagues in the minority believe the tag would preclude the analyst from accessing the information, then the new requirement would have immensurable operational impact on the agency's ability to fulfill its primary mission to analyze and disseminate foreign intelligence information.

(~~TS//SI//NF~~) *Third*, the recommendation would fundamentally alter how analysts think about traffic, requiring them to be on the lookout for U.S. person data early in data processing rather than trained on foreign intelligence information. And paradoxically for a Board with the mission to protect U.S. person privacy, the recommendation essentially calls for the creation of a database of USPI. One where USPI presumably would be, thanks to the new tag, easily accessible and searchable with the click of a button. For those reasons and more, I respectfully decline to join the recommendation.

(~~TS//SI//NF~~) *Minority Recommendation 3.* As explained in the Board's report, [redacted][3] By prioritizing foreign intelligence, the NSA *de facto* de-prioritizes other information, such as USPI containing no foreign intelligence.

(~~TS//SI//NF~~) Minority recommendation 3 asks the agency to affirmatively de-prioritize USPI. Yet, because information that contains USPI but no foreign intelligence already is *de facto* de-prioritized, the recommendation would seem to affect only information that contains *both* USPI *and* foreign intelligence. For that subset of information, one of two things must be true. Either the recommendation, if implemented, would have no impact, and the agency would prioritize the information as before. In which case the game seems not worth the candle. Or the recommendation would cause the information to be de-prioritized and, accordingly, potentially not ingested. In which case, the recommendation strikes me as substantively problematic: the NSA is authorized to collect foreign intelligence information, some of which will, inevitably, contain USPI. That is entirely expected, and is accounted for in executive branch and agency

[1] (U) DoDM at Section 3.3.f.(1)(b).2.
[2] (U) See the analysis from the Report in Section III.A on page 16.
[3] (U) *Id.*

procedures that implement privacy protections specific to USPI. Requiring the agency *not to collect* – and therefore not to be able to view or analyze – potentially valuable foreign intelligence information because it contains some (unspecified and unviewed) USPI would harm the agency's ability to conduct its mission within its lawful bounds. Before agreeing to a recommendation with the potential for such a sweeping effect, I would want to better understand its rationale, its operational impact, and whether any upside would outweigh the potentially vast cost of reworking the agency's extant technology for link collection.

Additional Classified Statement by Board Member Travis LeBlanc

(U) Introduction

(U) Today, I regretfully write in opposition to the release of a report that the former majority of the Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board") rushed last year to approve without adequate investigation, analysis, review, or process. While I remain grateful to our Board staff for the many years of effort they have devoted to XKEYSCORE's oversight, I had hoped that the former majority of the Board would have conducted a more thorough investigation of this highly-classified surveillance program that is unlikely to be scrutinized by another independent oversight authority in the near future.

(~~TS//SI//~~REL) XKEYSCORE is a software platform that enables the National Security Agency's ("NSA") signals intelligence ("SIGINT") analysts to conduct queries against communications data that NSA obtains [redacted][2] In that regard, I have no doubt that this sweeping surveillance program is worthy of our independent oversight. The mission of the Privacy and Civil Liberties Oversight Board is to ensure that the Executive Branch's efforts to protect the nation from terrorism appropriately safeguard privacy and civil liberties.[3] We do this best when we conduct a thorough investigation, review records that corroborate or contradict an agency's oral representations, probe compliance infractions, rely upon evidence-based analysis to reach independent conclusions, identify technological and legal evolutions that are material to the program's lawfulness, and produce a report that is as transparent to the public as possible. Today's report unfortunately fails along these metrics.

(~~TS~~) *First*, the Board attempts to explain an "analysis"[4] and "discovery"[5] tool, yet fails to inspect how XKEYSCORE obtains its information.[6] This is especially concerning [redacted] Obviously, NSA can process and query communications through XKEYSCORE only once it has access to those communications. While collection and querying are separate activities, they are intertwined and both are worthy of review for separate legal analysis, training, compliance, and audit processes. This is true whether the collection and querying activities are performed by humans or machines. What may be a reasonable amount of "incidental" collection in one program or activity may well be unreasonable in other contexts.[8] Similarly, protections that are designed to mitigate incidental collection may be

[1] (U) PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON CERTAIN NSA USES OF XKEYSCORE FOR COUNTERTERRORISM PURPOSES 1 (2021) ("NSA Deep Dive").
[2] (U) NSA Deep Dive at 1.
[3] (U) *See generally* 42 U.S.C. § 2000ee.
[4] (U) NSA Deep Dive at 1.
[5] (U) NSA Deep Dive at 2.
[6] (U) NSA Deep Dive at 13.
[7] (U) NSA Deep Dive at 18.
[8] (U) *See e.g.*, the surveillance conducted under a traditional wiretap as opposed to "upstream surveillance."

reasonable in one program or activity and unreasonable in other contexts. On these points and others, the former Board's report unfortunately reads more like a book report summary of the XKEYSCORE program than an independent oversight analysis grappling with key concerns in this evolving technological and legal landscape.

(U) *Second*, the Board had the opportunity to engage in evidence-based policy making; however, it concluded a report lacking analysis of the efficacy, costs, and benefits of XKEYSCORE.[9]

(~~TS//SI//NF~~) *Third*, the Board failed to adequately investigate the compliance program in place for XKEYSCORE. Unfortunately, it appears as if NSA had not prepared a written analysis of the legality of XKEYSCORE until prompted by the PCLOB.[10] Unsurprisingly, there was no mandatory XKEYSCORE training for NSA analysts, nor did the former Board majority agree to follow up on any of the [redacted] of compliance incidents that were reported to us.[11] The NSA reported, for example, that in 2019, there were [redacted] XKEYSCORE compliance incidents and that [redacted] these were deemed to constitute "Questionable Intelligence Activities"—a term used by the Department of Defense to signify that an action may have resulted in illegal surveillance or improper review of U.S. person communications.[12] But the Board refused to inquire into any of these compliance incidents or [redacted] U.S. person XKEYSCORE queries before issuing this report.[13]

(U//~~FOUO~~) *Fourth*, I joined fellow Board Member Ed Felten in offering three additional recommendations for the report.[14] These important recommendations involve [redacted] and the affirmative de-prioritization of U.S. person information.[15] These are three important recommendations that should have been adopted by the full Board.

(U) *Fifth*, the former majority has also failed its mission to inform the public about our work. Our authorization statute directs us to make our reports, including our reports to Congress, "available to the public to the greatest extent that is consistent with the protection of classified information and

---

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 7-8 (2014). *See also* DAVID KRIS AND J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 3:2 (3rd. ed. 2019).

[9] (~~TS~~) The report mentions NSA's various evaluative judgements on items such as [redacted] but asks no questions on metrics, when and why [redacted] and no discussion of data or variables. *See* NSA Deep Dive at 16. The lack of efficacy is in stark contrast to previous reports issued by PCLOB. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 63 (2020). *See also* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 2020 13 (2014); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 158 (2014).

[10] (U) *See* (~~S//NF~~) Nat'l Security Agency, *Legal Analysis of XKEYSCORE*, Jan. 20, 2016 at 5 ("NSA Legal Analysis").

[11] (U) NSA Deep Dive at 35.

[12] (U) Questionable Intelligence Activities (QIA) defined as "any intelligence or intelligence-related activity when there is reason to believe such activity is unlawful or contrary to an E.O., Presidential Directive, IC directive, or applicable DOD policy governing the activity." Department of Defense, *DOD Directive 5148.13: Intelligence Oversight* 16 ("DOD Directive 5148.13").

[13] (U) PCLOB Questions received on Sept. 14, 2020 regarding XKEYSCORE Deep Dive; Phone Call re: XKEYSCORE Dec. 14, 2020.

[14] (U) NSA Deep Dive at 50-51.

[15] (U) NSA Deep Dive at 50-51.

applicable law."[16] Here, the Board has made no effort to seek declassification of the report, any portions thereof, or any materials that the Board reviewed. This is inexcusable. Although the public will not have access to a public report, I plan to publish an unclassified statement to be released along with whatever version of the report is ultimately made public—even if the report is all or nearly all redacted. It is critical for the public to know that at least one Board Member has significant concerns about the operations of XKEYSCORE and the content of this report.

(U) *Lastly*, I have serious concerns about the unconventional process that the former majority followed to approve and release this report. To be clear, despite my repeated requests, the current Board has not voted to release this report nor to include the statement of a former member. The result is that today the former Board releases an inadequate report that reflects its failure to engage in effective oversight.

(U) Despite such critiques, I again commend the professional staff must be commended for their diligent, hard-working, and proficient work. They were critical to moving this report forward and I join my fellow Board Members in thanking them for their professionalism and their dedication to the Board's mission.

(~~TS//SI//REL~~) A Failure to Investigate

(~~TS//SI//REL~~) *First*, I voted against the XKEYSCORE report because the former majority failed to adequately investigate or evaluate NSA's collection activities [17] While XKEYSCORE itself is a software program capable of discovering and extracting signals intelligence, it is clear that NSA must gather or collect that signals intelligence from somewhere—in the United States or abroad. The former Board declined to review the agency's collection activities.[18] I disagree with that decision because

(~~TS//SI//REL~~)

[16] (U) 42 U.S.C. 2000ee(f)(1).

[17] (U) NSA Deep Dive at 18.
[18] (U) NSA Deep Dive at 18.
[19] (U) NSA Deep Dive at 18.
[20] (U) NSA Deep Dive at 18 n.32.
[21]

[redacted][22] The agency takes a one-size-fits-all compliance approach to the risks of "incidental" collection that relies upon its back-end minimization processes to address overcollection: "Any incidental U.S. person information will be handled consistent with the Classified Annex to the Department of Defense Manual 5240.01."[24] This, however, misses the point.

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

(~~TS//SI//REL~~) The enhanced risk to the privacy of U.S. persons whose communications may be intercepted incidentally are not just greater when [redacted] but also when NSA [redacted]

[22] [redacted]

[23] (U) Phone Call re: XKEYSCORE Dec. 14, 2020.

[24] (U) PCLOB Questions received on Sept. 14, 2020 regarding XKEYSCORE Deep Dive; Department of Defense, *Manual 5240.01. Procedures Governing the Conduct of Intelligence Activities* (2016).

[25] [redacted]

[26] [redacted]

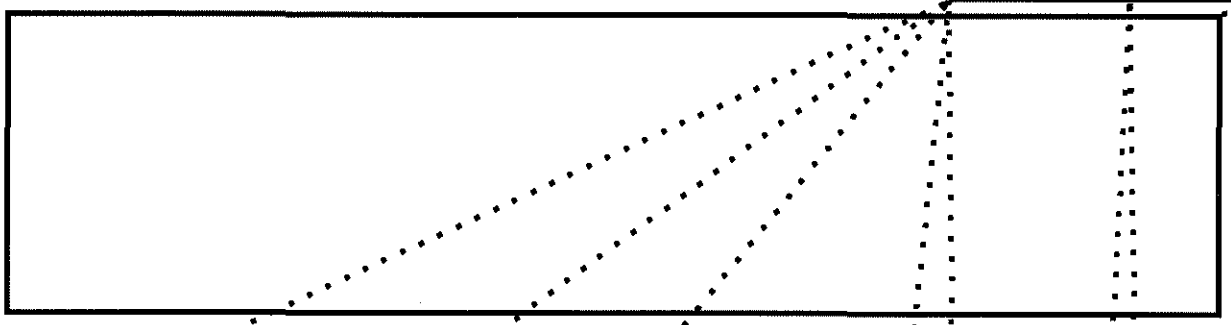
[27] (U) Phone Call re: XKEYSCORE Dec. 14, 2020.

[28] (U) NSA Deep Dive at 13-15.

[29] (U) NSA Deep Dive at 13-15.

[30] (U) NSA Deep Dive at 13.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



~~(TS//SI//REL)~~. The NSA and former Board majority disregard the risks associated with [redacted] and the associated harm to the privacy and civil liberties of U.S. persons as being indistinguishable from the risks and harms associated with [redacted]. As explained above, I disagree. In my view, the inability to address concerns around [redacted] are serious deficiencies with the report. The Board should have worked with NSA to analyze the likelihood of collecting U.S. person information at [redacted] recommended that the agency document whenever an analyst or other personnel becomes reasonably aware that U.S. person information is collected and/or analyzed from any collection site, and established appropriate minimization procedures before this data ever gets ingested into XKEYSCORE.

- The NSA's legal analysis and former Member Aditya Bamzai's exegesis[33] on the Fourth Amendment both disregard [redacted]

[31] (U) Phone Call re: XKEYSCORE Dec. 14, 2020.
[32] (U) NSA Deep Dive at 13-15.
[33] (U) I often urge my colleagues that we should exercise caution in expounding on the constitutional analysis of a program, particularly when the Supreme Court has not directly spoken to an issue. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 74 (2020). I do, however, feel compelled to reply to former Member Bamzai's statement where its conclusions could be misconstrued. For instance, it is my understanding that the Supreme Court has left open the question of whether there is a "foreign intelligence exception" to the Fourth Amendment. I am mindful to exercise caution in expanding any special needs exception to the Fourth Amendment. Such a malleable exception is at risk of not only expanding the Fourth Amendment beyond the expectations of the Founding Fathers, but also of expanding it beyond the literal text of the Amendment. Such an expansion risks sweeping into its ambit numerous activities solely because they are un-favored today. Thus, I tread cautiously and inspired by the wisdom of Justice Marshall, who wrote in *Skinner v. Railway Labor Executives' Association*, "There is no drug exception to the Constitution, any more than there is a communism exception or an exception for other real or imagined sources of domestic unrest. [A]bandoning the explicit protections of the Fourth Amendment seriously imperils; the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."' *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 604, 641 (1989) (Marshall, J., dissenting) (citation omitted) (quoting *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).
[34] (U) See *Statement of Former Board Member Aditya Bamzai*. While I appreciate the thoughtfulness that former Member Bamzai devoted to his Fourth Amendment analysis, it is worth noting the lack of any application of that analysis to the facts of XKEYSCORE.
[35] [redacted] (~~S//NF~~) NSA Legal Analysis at 5; [redacted] *See generally Statement of Former Board Member Aditya Bamzai*.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (5)

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(~~TS//SI//REL~~)

(~~TS//SI//REL~~)

[36] (~~TS~~) Former Member Bamzai begins his discussion by relying on as well as *United States v. Verdugo-Urquidez* where the central issue was a warrantless search of a non-resident person outside the United States. *See Statement of Former Board Member Aditya Bamzai* at 3-4.

[37] (U) NSA Deep Dive at 18.

[38] (U) NSA Deep Dive at 18.

[39] (U) NSA Deep Dive at 18.

[40] (U)

[41] (U) NSA Deep Dive at 18.

[42] (U)

[43] (U)

[44] (U) NSA Deep Dive at 18. *See*

[45] (U)

[46] (U)

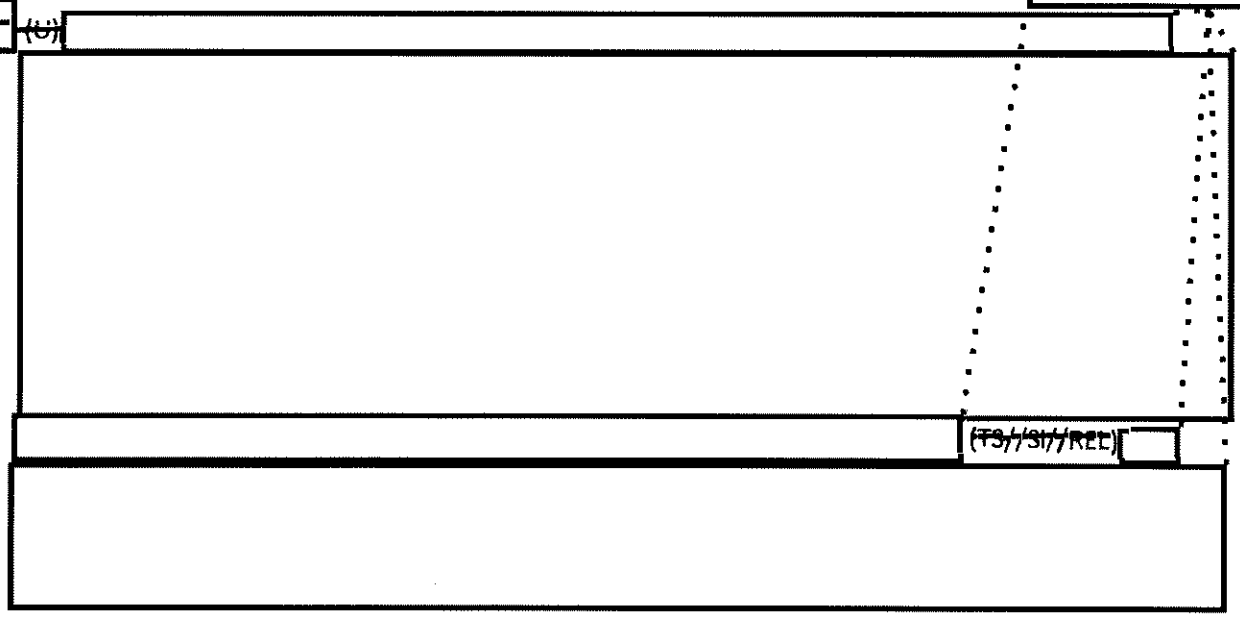
[47] (U) NSA Deep Dive at 18.

(b) (3)-P.L. 86-36
(b) (5)

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (5)

~~TS//SI//REL~~ (U)



~~(S)~~ Setting aside the legal distinctions between the XKEYSCORE collections and Title III or traditional FISA collections, the capabilities of modern electronic surveillance are more vast than the technologies discussed 40-50 years ago in *Smith v. Maryland* and *Katz v. United States*.[56] Any legal analysis must account for how these new capabilities create emerging privacy harms, which themselves pose new legal challenges: for example, the extent to which machine surveillance is the same as human surveillance; the extent to which the aperture of collection and amount of data intercepted fundamentally alter the reasonableness analysis; the extent to which the Mosaic Theory is implicated, and how to apply recent Supreme Court decisions in digital surveillance cases like *Carpenter v. United States* and *Riley v. California*.[57]

~~(S)~~ All of the cases relied upon by former Member Bamzai assume the Fourth Amendment is triggered once a human reviews intercepted communications.[58] The unstated assumption is that machine collection and analysis of U.S. person communications does not trigger the Fourth Amendment until a

[48] (U) *Statement of Former Board Member Aditya Bamzai* at 6-7, 9; (~~S//NF~~) NSA Legal Analysis at 5.
[49] (U) *Seee.g.*,
[50] (U) NSA Deep Dive at 13-15.
[51] (U) NSA Deep Dive at 25.
[52] (U) *See* the surveillance at issue in
[53] (U)
[54] (U)
[55] (U)
[56] (U) *Smith v. Maryland*, 442 U.S. 735 (1979); *Katz v. United States*, 389 U.S. 347 (1967).
[57] (U) *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373, 381 (2014).
[58] ~~(S)~~ Former Member Bamzai appears to provide an analysis resting on traditional electronic surveillance concepts and capabilities where the government collects information from one telephone line with two communicants.

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36
(b) (5)

human actually reviews those communications, or at least, the communications that are flagged by the machine for subsequent human review. My concern, however, is that the machine's review is the substantial equivalent of a human review, albeit vastly more efficient. That the machine flags only suspicious communications does not mean that the intrusion is any less for all the other communications or if they had all been reviewed by a human. Thus, the question presents itself of whether the Fourth Amendment can be trigged by a government (human)-directed-but-machine-operated collection and analysis tool–even if it does not directly result in a flag of suspicion for immediate human review. As surveillance technologies have evolved, massive volumes of bulk data can be processed efficiently and at a scale that would be impossible or absurdly impractical for humans to perform. This can be even more invasive from a Mosaic Theory framework when machines are efficiently amassing and analyzing disparate data.[59] it stands to reason that algorithms are not separate entities from their human overseers.[60] When a human creates, directs, or instructs an algorithm, the algorithm is acting as a government actor engaged in the collection and search of intercepted communications. Thus, there are two independent analyses that should have been performed in the XKEYSCORE context: one involving collection and the other involving querying with a recognition of the role of machines in triggering Fourth Amendment scrutiny. In the XKEYSCORE context, this means that a revaluation of the Fourth Amendment consequences should be analyzed at the point of initial collection

(TS//SI//REL) XKEYSCORE is one tool that NSA has available for its human and machine analysts to efficiently digest As the report notes, XKEYSCORE With access to such the privacy risks associated with even disparate collection of seemingly banal information

---

Nowhere is there a discussion by former Member Bamzai on the unique technical aspects of XKEYSCORE collection. *Statement of Former Board Member Bamzai at 5* citing "I believe the same basic analysis remains relevant today."); *See also* former Member Bamzai's reliance on cases like *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990); *United States v. Donavan*, 429 U.S. 413 (1977); *United States v. Kahn*, 415 U.S. 143 (1974). *Statement of Former Board Member Bamzai at 5*. Even when former Member Bamzai discusses more recent case law regarding Section 702 surveillance, there is little analysis of the initial surveillance collecting the communications at issue nor the breadth and depth of "upstream surveillance" as released in the Board's *Report on the Government Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2014). *Id.;* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 158 (2014). Former Member Bamzai is singularly focused on post-acquisition protections: "Ultimately, this analysis [in whether XKEYSCORE complies with the Fourth Amendment] likely turns on whether NSA adequately protects any U.S.-person communications processed by XKEYSCORE from misuse." *Statement of Former Board Member Bamzai* at 17.

[59] (U) Orin S. Kerr, *The Mosaic Theory and the Fourth Amendment*, MICH. L. REV. 111:311-354 (2012); Paul S. Ohm, *The Many Revolutions of* Carpenter, HARVARD J. OF L. AND TECH. 32:358-416 (2019); Danielle Citron and David Gray, *The Right to Quantitative Privacy*, MINN. L. REV. 98:62-144 (2013).

[60] (U) FRANK PASQUELE, BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION, HARVARD UNIVERSITY PRESS (2015). *See also* Danielle Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

[61] (U) NSA Deep Dive at 25.

[62] (U) *Id.*

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

are present: "[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene."[63] The ability to sample significant amounts of data; send the data to a database with an analytical tool; have that analytical tool monitor all information ingested into it; and then have the analytical tool assist human analysts to review retrospective communications, email attachments, metadata, and other information is profound.[64]

~~(TS//SI//REL)~~ [redacted] scholars have noted that predictive algorithms pose unique harms to privacy interests.[66] Many of these algorithms automate the process of identifying suspicious individuals from data.[67] Artificial intelligence and machine learning act as a steroid of sorts allowing for humans to increase both their breadth and depth of surveillance. Artificial intelligence and machine learning concepts like autonomous discovery and targeting of data as well as predictive decision making could serve as an all-seeing eye presenting new, unique privacy and civil liberties harms.

~~(TS//SI//REL)~~ Unfortunately, former Member Bamzai's Fourth Amendment analysis fails to account for the factors that make XKEYSCORE different from other surveillance technologies considered by courts in the last century.[68] Factually, it incorrectly assumes that [redacted][69] Legally, it glosses around Fourth Amendment issues at the point of collection, machine surveillance, and the impact that the Mosaic Theory and more recent case law around digital surveillance have on programs like XKEYSCORE.[70]

(U) A Failure to Investigate: Cost-Benefit Analysis and Efficacy of the Program

~~(TS)~~ *Second*, it is basic that oversight of a government program should include an evaluation of the efficacy of the program, including at least an analysis of its costs and benefits.[71] I voted against the report because the former Board failed to evaluate the efficacy of XKEYSCORE through a cost-benefit analysis or otherwise. In the past, the Board has included an efficacy analysis in all three of the major

[63] (U) *CIA v. Sims*, 475 U.S. 159 (1985); *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).
[64] (U) It is even more profound in light of the Mosaic Theory. *See* (U) Orin S. Kerr, *The Mosaic Theory and the Fourth Amendment*, MICH. L. REV. 111:311-354 (2012); Paul S. Ohm, *The Many Revolutions of* Carpenter, HARVARD J. OF L AND TECH. 32:373-73; Danielle Citron and David Gray, *The Right to Quantitative Privacy*, MINN. L. REV. 98:62-144 (2013).
[65] (U) [redacted]
[66] (U) *Id. See also* Michael L. Rich, *Machine Learning, Automated suspicion Algorithms, and the Fourth Amendment*, U. PENN L. REV. 164:872 (2016).
[67] (U) See *id.*
[68] (U) *See supra n.50.*
[69] (U) *See supra n.27.*
[70] (U) *See supra n.55.*
[71] (U) Council of the Inspectors General on Integrity and Efficiency, *Quality Standards*, https://www.ignet.gov/content/quality-standards.

(b) (3)-P.L. 86-36

oversight reports that we have released.[72] One would expect that after five years of investigating XKEYSCORE, the former majority would have some sense—even a rough one—of how much the program costs financially to operate, how many U.S. persons have been impacted by XKEYSCORE, how much data the program collects and analyzes, how widely information analyzed through XKEYSCORE is shared, the number of lives saved, the number of terrorist events averted as a result of XKEYSCORE, or at least have more than just two counterterrorism examples of the "Operational Value" of the program, particularly given how "powerful, ingenious, adaptable, and customizable" a tool at least one Member apparently concludes that it is.[73]

(~~TS//SI//REL~~) Effective oversight necessitates a robust investigation into the efficacy of the programs we oversee. The Board's former majority has failed to do that. To accept two examples of "Operational Value"[74] and conclude confidently that XKEYSCORE is "highly effective"[75] is incredible, especially when the former Board never investigated what makes a "highly effective" surveillance tool and the former Board has not defined what it would take to constitute such a success. Indeed, when I insisted that we ask the NSA to consider what statistics or descriptions they could provide to address the "cost and value" of XKEYSCORE, the agency admitted that it had not performed any such analysis and that "it would be difficult to pinpoint any one cost or benefit" of the program.[76] We should not have prematurely terminated our investigation of efficacy to rush to a vote on this report before the end of 2020. The former Board, along with the NSA, could have, and should have, engaged in a robust dialogue on the metrics, variables, and key computational questions concerning the efficacy and effectiveness of this "powerful" surveillance tool.[77] Unfortunately, that dialogue and evidence-based policy analysis did not occur.

(U) The Lack of a Robust Compliance Program

(U) *Third*, I voted against the report because the former Board majority sought to issue it without completing diligence on NSA's compliance efforts, including its legal analysis, policies, training, compliance, and auditing.

(U//~~FOUO~~) A primary step in any compliance program is a legal analysis of the program.[78] The legal analysis that sets forth the authorities and limitations of a program typically forms the foundational basis necessary for the development of compliance policies and procedures. Surprisingly, NSA apparently did not draft any formal legal analysis of the program until asked by the former Board in

[72] (U) PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT, 2020 13 (2014); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 158 (2014); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 63 (2020).

[73] (U) *Additional Views by Chairman Adam Klein* at 1.

[74] (U) NSA Deep Dive at 29.

[75] (U) *Additional Views by Chairman Adam Klein* at 1.

[76] (U) NSA Correspondence with PCLOB, Sept. 21, 2020.

[77] (U) *Additional Views by Chairman Adam Klein* at 1.

[78] (U) *See generally* INT'L ASSN. OF PRIVACY PROFESSIONALS, PRIVACY PROGRAM MANAGEMENT (2nd. ed. 2019); Nat'l Institute of Standards and Tech., *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, 11 (Jan. 16, 2020).

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

2015.[79] It is, of course, concerning that a surveillance tool as "powerful" as XKEYSCORE was conceptualized, coded, implemented, and then executed without any initial written legal analysis.[80]

(U//~~FOUO~~) Setting aside that NSA's legal analysis was first written in January 2016, it is equally concerning that the agency apparently has not updated that written legal analysis since then.[81] The 2016 analysis fundamentally rests on decades-old Supreme Court precedent from *Verdugo-Urquidez*, *Smith*, *Katz* and two DOJ legal memoranda from the 1980s to assert that collection and use of XKEYSCORE is consistent with the Fourth Amendment.[82] The 2016 analysis lacks an analysis of recent relevant Fourth Amendment case law on electronic surveillance: *Carpenter*, *Riley*, *United States v. Jones*, *and United States* v. *Maynard* need to be considered.[83]

(~~TS//SI//REL~~) The 2016 analysis also fails to discuss

(U) The deficiencies in NSA's legal analysis were as apparent to the former Board as they are to me. Thus, I am glad that the former Board has recommended that NSA update its legal analysis and identified several key constitutional and legal issues that NSA should consider when it does prepare a satisfactory legal analysis of the XKEYSCORE program.[85]

(U//~~FOUO~~) Given the apparent lack of a legal analysis prior to our investigation, it should come as no surprise that NSA does not currently require analysts to receive privacy and civil liberties compliance training tailored to XKEYSCORE.[86]

(~~S//SI//REL~~) While NSA does require all personnel with the ability to review raw SIGINT data to complete online training and competency testing prior to accessing data in XKEYSCORE, the privacy and civil liberties components of those trainings are minimal and not specific to XKEYSCORE.[87] NSA's optional XKEYSCORE-specific trainings are equally deficient in their treatment of privacy and civil liberties.[88]

---

[79] (U) The former Board asked NSA to provide any "[l]egal analysis by the NSA and Department of Justice regarding the use of XKEYSCORE's analytic functions and its consistency with statute, executive order, and the Constitution." PCLOB Document Request to NSA, Dec. 15, 2015.

[80] (U) *Additional Views by Chairman Adam Klein* at 1.

[81] (~~S//NF~~) NSA Legal Analysis.

[82] (U) *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990); *Smith v. Maryland*, 442 U.S. 735 (1979); *Katz v. United States*, 389 U.S. 347 (1967); (~~TS//SI//NF~~

[83] (U) *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

[84] (~~S//NF~~) NSA Legal Analysis.

[85] (U) NSA Deep Dive at 46.

[86] (U) NSA Deep Dive at 35.

[87] (U) NSA Deep Dive at 35 n.72 and 73.

[88] (U) NSA Deep Dive at 35.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

(U//~~FOUO~~) One would have expected, however, that there would be mandatory, robust compliance training tailored to XKEYSCORE given how powerful of a tool it is.

(~~S//SI//REL~~) I am pleased that my colleagues have recommended that NSA mandate specific XKEYSCORE compliance training.[89] But this recommendation does not go far enough in my view. The recommendation unfortunately provides no guidance on the content of that training, which should, at a minimum, include a presentation on the privacy risks associated with the collection and handling of U.S. person information, limitations on the collection and querying of U.S. person information, compliance standards for XKEYSCORE queries [redacted]. Analysts should also be required to retrain on XKEYSCORE compliance periodically—whether after an identified time period has elapsed, after a serious compliance incident (such as a Questionable Intelligence Activity),[90] after a substantial update to XKEYSCORE's capabilities, and/or upon legal developments (such as new judicial precedent or a relevant change to an NSA policy) warranting further instruction on compliance.

(~~S//REL~~ S//~~FOUO~~) Additionally, I am troubled that the former Board majority failed to investigate [redacted] of serious compliance incidents involving XKEYSCORE prior to approving the report. During the former Board's investigation, we learned in November 2020 that [redacted] compliance incident reports occurred in 2019.[91] Of those [redacted] XKEYSCORE incidents, [redacted] were deemed upon agency review to involve activities that may have violated law or NSA policy, also known as a Questionable Intelligence Activity or "QIA."[92] That is over [redacted] of incident reports in a one-year period. Obviously, violations of U.S. law and the known collection or processing of U.S. person information are serious compliance issues. Yet, the former majority did not request information on any of these [redacted] QIAs prior to approving the report, nor did the former Board request equivalent data about compliance incidents in any other year.[93]

(~~TS//SI//NF~~) Compliance questions persist beyond the issue of QIAs. For instance, the former Board also uncovered that over [redacted] U.S. person queries were conducted through XKEYSCORE in only a 9 month period between January 2020 and September 2020.[94] While NSA represented that the searches were mostly [redacted] the agency could not provide the former Board with the legal justifications for each of these queries because "NSA would have to manually review all [redacted] justifications . . . and categorize them."[95] The former Board should have sought a manual review of the [redacted] U.S. person queries, or, at least reviewed a subset of these U.S. person queries before issuing its

[89] (U) NSA Deep Dive at 48.

[90] (U) Questionable Intelligence Activities (QIA) defined as "any intelligence or intelligence-related activity when there is reason to believe such activity is unlawful or contrary to an E.O., Presidential Directive, IC directive, or applicable DOD policy governing the activity." *DOD Directive 5148.13* at 16.

[91] (U) PCLOB Questions received on Sept. 14, 2020 regarding XKEYSCORE Deep Dive, Answer 2(b)(i); See also NSA Briefing on XKEYSCORE (Feb. 7, 2019).

[92] (U) PCLOB Questions received on Sept. 14, 2020 regarding XKEYSCORE Deep Dive. *See supra* n.90.

[93] (U) The behavior is in stark contrast to the former Board's approach in its 2020 *Report on the Government's Use of the Call Detail Records Program Under the USA Freedom Act* where it engaged in rigorous analysis into the efficacy of the program. There, the Board dedicated an entire section of the report to discussing compliance incidents: "Root Causes of the Compliance Incidents and Date Integrity Challenges." *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 63 (2020).

[94] (U) PCLOB Questions received on Sept. 14, 2020 regarding XKEYSCORE Deep Dive.

[95] (U) PCLOB Questions received on Sept. 14, 2020 regarding XKEYSCORE Deep Dive.

(b) (1)
(b) (3)-P.L. 86-36

report. The lack of follow-up on [redacted] compliance incidents and [redacted] of U.S. person queries are deeply concerning for an oversight Board tasked with ensuring "that privacy and civil liberties are appropriately considered in the development and implementation of legislation, regulation, policies, and guidelines" to protect the nation from terrorism.[96]

~~(U)~~ The lack of satisfactory legal analysis, insufficient training, [redacted] of compliance reports, and the former Board's inability to investigate critical privacy and civil liberties issues all shine poorly on the former Board's credibility and ability to conduct itself as an oversight body. It is disheartening that the former majority has failed to conduct this basic oversight in a rush to publish this report.

(U) The Board Failed to Adopt the Minority Recommendations

~~(TS//SI//NF)~~ *Fourth*, the former Board's report fails to adopt three important recommendations that Board Member Felten and I submitted involving NSA's capacity [redacted] and the affirmative de-prioritization of U.S. person information.[97]

(b) (3)-P.L. 86-36

(U//~~FOUO~~) I join Member Felten's discussion of our additional recommendations in his separate statement and also note that while inadvertently or incidentally intercepted communications of U.S. persons is a casualty of modern signals intelligence, the mere inadvertent or incidental collection of those communications does not strip affected U.S. persons of their constitutional or other legal rights.[98] Even NSA's Legal Compliance and Minimization Procedures (United States Signals Intelligence Directive SP0018) recognize that inadvertently collected U.S. person communications "will be promptly destroyed upon recognition, if technically possible" (except in a few enumerated circumstances such as a threat of death or serious bodily harm).[99] Setting aside whether known U.S. person communications should be retained at all, Member Nitze apparently takes issue with the minor effort that it would take for an analyst to tag data known or believed to constitute U.S. person information [redacted] that may be retained and queried for five years (as of now).[100] Member Nitze does not argue that the tagging requirement she opposes would be unreasonable or unduly burdensome on analysts.[101] Nor could she. The recommendation does not require NSA analysts to take any actions in seeking to identify U.S. person information, nor does it require NSA to substantively amend its minimization procedures.[102] But as the NSA has itself explained, "NSA is required by its Attorney General approved minimization procedures to make reasonable efforts to reduce to the maximum extent practicable the number of non-foreign communications acquired during SIGINT operations."[103] The creation and use of a U.S. person

---

[96] (U) 42 U.S.C. § 2000ee(c)(2).
[97] (U) NSA Deep Dive at 50-51.
[98] (U) U.S. v. *Warshak*, 631 F.3d 266 (2010); *Berger v. New York*, 388 U.S. 41, 59 (1967); *Katz v. United States*, 389 U.S. 347 (1967); 18 U.S.C. § 2518; 50 U.S.C. § 1805, § 1824.
[99] (U) Nat'l Security Agency, *United States Signals Intelligence Directive SP0018: Legal Compliance and U.S. Persons Minimization Procedures* § 5.4(b)(1), Jan. 25, 2011 ("USSID 18").
[100] (U) *Statement of Board Member Janie Nitze* at 1.
[101] (U) *Statement of Board Member Janie Nitze* at 1.
[102] (U) NSA Deep Dive at 50-51.
[103] ~~(S//NF)~~ NSA Legal Analysis at 7.

information tag is clearly reasonable and this is particularly so when the objective is to reduce the collection and retention of U.S. person communications to the *maximum extent possible.*

~~(TS//SI//NF)~~ It is also equally apparent that communications an analyst knows or reasonably believes to constitute U.S. person information should be treated as such. Member Nitze postulates, "[W]hat is an analyst to do if he is pretty sure, but not certain, that information is 'US person data'?"[104] My answer is simple: tag it as U.S. person information. We can easily draw from familiar common law or Section 702 principles (for example) to understand that tagging should occur upon a reasonable belief that that the communication includes U.S. person information; certainty is not required.[105]

(U) Even the NSA concurs, "A person known to be currently outside the UNITED STATES, or whose location is not known, will not be treated as a U.S. PERSON unless such person is reasonably identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such a person is a U.S. PERSON."[106]

~~(TS//SI//NF)~~ Of course, the tagging of communications as U.S. person information is not a license to create a "database of USPI" as Member Nitze seems to fear.[107] Recommendation 2 intends to minimize U.S. person information from being analyzed by XKEYSCORE, reviewed by additional NSA analysts, retained in violation of controlling legal authorities, and inappropriately disseminated to other agencies. Given that NSA has implemented minimization procedures and also complies with Section 309 of the Intelligence Authorization Act of 2015, the agency should put in place a compliance process to review the tagged communications and appropriately dispose of them or otherwise minimize the sharing of those communications.[108] The recommendation would require NSA analysts to ensure U.S. person information reasonably known to them is tagged.[109] Once that is done, NSA's existing compliance and auditing system could apply itself. Incidentally, I note that the mandatory tagging of U.S. person information will also have utility for compliance and oversight insofar as there will be data on the prevalence of U.S. person information processed through XKEYSCORE—an estimate NSA is apparently unable or unwilling to provide today.[110]

~~(TS//SI//NF)~~ The third recommendation that Member Felten and I issued seeks to mitigate the harm of incidental U.S. person collections by requiring NSA to affirmatively de-prioritize U.S. person information processed by XKEYSCORE.[111] Although Member Nitze objects to this recommendation, the mere fact that [redacted]

[redacted]

[104] (U) *Statement of Board Member Janie Nitze* at 1.
[105] (U) Nat'l Security Agency, *FISA Section 702 Minimization Procedures* § 2(k)(2) (2015).
[106] (U) USSID 18 § 9.18(e)(2).
[107] (U) *Statement of Board Member Janie Nitze* at 2.
[108] (U) Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 119-213 (2014); *See generally* USSID 18.
[109] (U) NSA Deep Dive at 50-51.
[110] (U) PCLOB Questions received on Sept. 14, 2020 regarding XKEYSCORE Deep Dive.
[111] (U) NSA Deep Dive at 50-51.
[112] (U) *Statement of Board Member Janie Nitze* at 2.
[113] (U) NSA Deep Dive at 16 n.24.

The NSA now apparently uses [redacted][114] Given the massive amount of data that XKEYSCORE digests, I believe our modest proposal to affirmatively de-prioritize U.S. person information is a reasonable protection against the privacy risks associated with incidental collection.

(U) The Board Failed the Public

(U) *Fifth*, the former majority of the Board has also failed in its mission to inform the public about our work. Our authorization statute directs us to make our reports, including our reports to Congress, "available to the public to the greatest extent that is consistent with the protection of classified information and applicable law."[115] Here, the Board has made no effort to seek declassification of this report, any portions thereof, or any materials that the Board reviewed. This is inexcusable. Although the public is not apparently expected to have access to any of the report, I will publish an unclassified statement to be released along with whatever version of the report is ultimately made public—even if the report is all or nearly all redacted. It is critical for the public to know that at least one Board Member has significant concerns about the content of this report and the operations of the program.

(U) In addition to our statutory mandate, there are very good policy reasons for why our Board's activities should be as transparent as possible. Transparency encourages accountability. When the PCLOB publicly releases its reports, it allows the public and other external stakeholders to engage with material that is often kept under classification and out of the public eye. It allows academics and journalists to further investigate potentially wasteful or unlawful government surveillance. It allows civil society to advocate for new policy positions. And it allows Congress to further oversee and legislate changes to the law. All of these actions engender public trust that there is sufficient and adequate oversight of national security programs and activities.

(U) The public is rightfully worried about secret surveillance programs. By being transparent with our reports and activities, PCLOB ensures the public understands oversight is occurring and that privacy and civil liberties harms are being addressed.

(U) Transparency encourages credibility. A thorough report increases PCLOB's credibility to provide constructive criticism to agencies engaged in practices with a potential for significant privacy and civil liberties harms. It also encourages credibility in NSA itself as the agency listens, responds, and incorporates feedback—not just from the Board, but from an informed democracy. It is unfortunate the Board has failed to seek declassification of even discrete sections of this report. As we have been directed by Congress, I urge the Board to request declassification of its report and release as much information to the public "to the greatest extent that is consistent with the protection of classified information and applicable law."[116]

[114] (U) NSA Deep Dive at 16 n.24.
[115] (U) 40 U.S.C. § 2000ee(f)(1).
[116] (U) *Id.*

(U) Procedural Issues Plague the Report

(U) Finally, I have several concerns about the Board process that was followed to apparently approve the unfinished report. In a December 2020 Board meeting, the former majority sought to vote on the then-unfinished XKEYSCORE report. During the Board meeting at which the vote was taken, we spent several hours discussing the revisions to the body and recommendations that would need to be made to the report. Instead of completing those revisions and then providing sufficient time for Members to review the report and prepare their statements before voting, the former Board majority sought in that meeting to approve the report for this project, ostensibly foreseeing the expiration of former Member Bamzai's term at the end of December. Literally on the evening of December 31, former Member Bamzai circulated his statement. Subsequently, the new Board convened in January and the Chairman submitted his own intention to resign the same month (although he has not departed the agency thus far). Recognizing that the current Board has not voted on a report that we are still considering for revision as I draft this statement, I have repeatedly requested a vote by the current Board on the final version of this report, including all final statements of current Members as well as a vote on whether to include the statement of a former Member. The current Chairman has created a legal fiction to compel the issuing of a former Member's statement without so much as a vote of the current Board or a vote of the current Board to release this report. I simply cannot support a report that has not been voted on by the current Board that will issue it.

(U) Conclusion

(U) For these reasons, I am unable to support this report. I hope the critical deficiencies and gaps identified in my statement will help provide guidance to NSA on additional issues that it needs to address with respect to the operations of XKEYSCORE. I also hope that the issues raised in this statement inspire a future PCLOB to more effectively perform its oversight and advising functions when assessing other surveillance programs.

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

(b) (3)-P.L. 86-36
(b) (5)

Separate Statement of Member Aditya Bamzai

(~~TS//SI//NF~~) I join in full the Board's Report on XKEYSCORE.[1] I write separately to address the legal questions raised by the capabilities described in this Report and to provide a conceptual framework for the Fourth Amendment analysis that the Report recommends the NSA undertake. The analysis that the NSA provided to the Board[2] to justify the legality of XKEYSCORE relies on

(~~TS//SI//NF~~) Decades have passed since

My analysis below addresses the more-recent case law, as well as the nuances that those cases raise.

[1] (~~TS//SI//REL~~)

[2] (~~TS//SI//NF~~) *See* NSA, *Legal Analysis of XKEYSCORE* (Jan. 20, 2016) ("NSA Legal Analysis") (created for PCLOB in response to the Board's request for any legal analyses written about XKEYSCORE).

[3] (~~TS//SI//NF~~) The NSA Legal Analysis also briefly notes that

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

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

1

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (5)

(b) (1)
(b) (3)-P.L. 86-36
(b) (5)

I.

(U) To start at the beginning, the Fourth Amendment provides:

> 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.[6]

By its terms, the Fourth Amendment thus contains a general prohibition on "unreasonable searches and seizures," as well as a requirement that "Warrants" be issued only under certain conditions—namely "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." I will call the prohibition on "unreasonable searches and seizures" the Fourth Amendment's "Reasonableness Clause," and the provision setting forth requirements for warrants the Fourth Amendment's "Warrant Clause."

(~~S//REL~~) Against this textual backdrop, two possible Fourth Amendment frameworks might bear on the legality of the collection of the type of information at issue in the uses of XKEYSCORE analyzed in the Board's Report. Under the first framework, the type of information collected for analysis using XKEYSCORE (or the manner of its collection) might fall outside of Fourth Amendment protection altogether. To put this point slightly differently, certain activities conducted by the government, though they may qualify as "searches" and "seizures" colloquially understood, fall outside the scope of the Fourth Amendment's protection—say, because they involve searches of non-U.S. persons conducted overseas.[7] Such government activities might be subject to neither the Fourth Amendment's Reasonableness Clause nor its Warrant Clause.

(~~S//REL~~) Under the second framework, an exception to the Fourth Amendment's Warrant Clause might apply to the type of collection at issue in the Board's Report and analyzed using XKEYSCORE, leaving the Fourth Amendment's "Reasonableness Clause" applicable. To put this point slightly differently, the type of collection at issue in the context of XKEYSCORE might not require a warrant under the Fourth Amendment, but might still have to satisfy the general prohibition against "unreasonable" searches and seizures.

---

[6] (U) U.S. CONST. amend. IV.

[7] (U) The term "United States person" is defined in several sources of law. *See* Executive Order No. 12,333 § 3.5(k) (defining the term to mean "a United States citizen," "an alien known by the intelligence element concerned to be a permanent resident alien," "an unincorporated association substantially composed of United States citizens or permanent resident aliens," or "a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments"); 50 U.S.C. § 1801(i) (defining the term to mean "a citizen of the United States, an alien lawfully admitted for permanent residence [in the United States], . . . an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States," unless such an association or corporation "is a foreign power").

(~~S//REL~~) In my view, it seems doubtful that all of the content collected for analysis using XKEYSCORE is outside Fourth Amendment protection altogether. For clarity, I nevertheless briefly address that possibility in Part II. It is more likely that the collection and analysis of XKEYSCORE is not subject to the Warrant Clause, but is subject to the Reasonableness Clause. I therefore address the proper framework for analyzing this issue in more detail in Part III.

II.

(~~S//REL~~) For purposes of clarity and comprehensiveness, I will start by discussing the possibility that neither the Warrant Clause nor the Reasonableness Clause applies in the XKEYSCORE context because of the extraterritorial exception to the Fourth Amendment identified in *United States v. Verdugo-Urquidez*.[8] As I explain below, I ultimately conclude that this approach is unlikely to provide a complete and satisfactory answer.

(U) In *Verdugo-Urquidez*, the Supreme Court held that the Fourth Amendment does not apply "to the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country."[9] The case therefore held that neither the Fourth Amendment's procedures for warrants, nor the Fourth Amendment's general requirement of reasonableness, applied in the circumstances at issue. At the same time, the case concerned the warrantless search of the residence in Mexico of a citizen and resident of Mexico, who had been brought to the United States for prosecution.[10] It therefore did not specifically address the incidental collection of any U.S. person information, nor did it address the collection within the United States of non-U.S.-person communications abroad.

(~~TS//SI//NF~~) In some respects, *Verdugo-Urquidez* did not break new ground. Six years before the Court decided *Verdugo-Urquidez* in the context of physical home searches,

[redacted][11]

(b) (3)-P.L. 86-36
(b) (5)

[8] (U) 494 U.S. 259 (1990).

[9] (U) *Id.* at 261; *cf. United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 318 (1936) ("Neither the Constitution nor the laws passed in pursuance of it have any force in foreign territory unless in respect of our own citizens."). As the Court's opinion in *Verdugo-Urquidez* indicates, the Court's holding appears to be consistent with early practice under the Fourth Amendment with respect to the seizure of foreign vessels in non-United States territory. *See* 494 U.S. at 267-68 (describing how, seven years after the Fourth Amendment's adoption, the United States engaged in an "undeclared war" with France following "French interference with American commercial vessels," for which Congress enacted a statute authorizing the President to "instruct the commanders of the public armed vessels which are, or which shall be employed in the service of the United States, to subdue, seize and take any armed French vessel, which shall be found within the jurisdictional limits of the United States, or elsewhere, on the high seas") (quoting An Act Further to Protect the Commerce of the United States, ch. 68 § 1, 1 Stat. 578, 578 (1798)).

[10] (U) *See* 494 U.S. at 262.

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

(b) (3)-P.L. 86-36
(b) (5)

(~~TS//SI//NF~~)

[12] As I will discuss further below, more recent cases have also concluded that the Reasonableness Clause, but not the Warrant Clause, applies to the incidental collection of U.S. person communications abroad.[13]

(U) As a result, the application of the extraterritoriality exception to both the Reasonableness *and* Warrant Clauses of the Fourth Amendment under *Verdugo-Urquidez* depends on a predictive judgment of the likelihood that Fourth-Amendment-protected information will be collected along with information outside the scope of the Fourth Amendment's protections. Where such collection is unlikely, the targeting of non-Fourth-Amendment-protected information would be outside the scope of the Fourth Amendment's warrant and reasonableness requirements. Where such collection is more likely, then the targeting might be subject to both or, if an exception to the warrant requirement is applicable, to the reasonableness requirement alone.

(~~TS//SI//NF~~)

(~~TS//SI//NF~~) In other words,

(b) (1)
(b) (3)-P.L. 86-36
(b) (5)

[12] (~~TS//SI//NF~~)
[13] (U) *See infra* Part III.B.1.
[14] (~~TS//SI//NF~~)
[15] (~~TS//SI//NF~~) *Id.*
[16] (~~TS//SI//NF~~) *Id.*

Id.

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

[redacted][18]

(U) I believe the same basic analysis remains relevant today. Some overseas searches and seizures of non-U.S. persons may fall outside the protections of the Fourth Amendment altogether under *Verdugo-Urquidez*. Where it is anticipated that U.S. person communications might be intercepted, however, the proper analysis requires application of the Fourth Amendment—to which I turn below.

(b)(3)-P.L. 86-36
(b)(5)

III. [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(5)

(~~TS//SI//NF~~) Because I understand that it can be anticipated that some U.S. person communications might be intercepted and then analyzed using XKEYSCORE, it is necessary to address the more comprehensive Fourth Amendment framework applicable to these circumstances. Written decades ago [redacted][20]

(~~TS//SI//NF~~) I believe [redacted] (1) the nature of incidental collection, (2) the extraterritorial and foreign intelligence "exceptions" to the Fourth Amendment's Warrant Clause, and (3) the appropriate analysis under the Reasonableness Clause. I discuss the three in turn.

---

[18] (~~TS//SI//NF~~) Approaching the question from the vantage point of a "predictive judgment" is consistent with the mainstream view that Fourth Amendment analysis is conducted from an *ex ante* perspective, assessing "whether a proposed investigatory activity was reasonable *given what the government knew at the time*, rather than with the benefit of hindsight." PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 41 (Feb. 2020); *see also Anderson v. Creighton*, 483 U.S. 635, 639 (1987). [redacted]

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

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

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

(b)(3)-P.L. 86-36
(b)(5)

A.

(~~TS//SI//REL~~) To the extent that the collection analyzed in XKEYSCORE might involve U.S. person information, the legality of such warrantless collection must depend on the concept of "incidental interception."[21] Because the program's *purpose* is to find foreign communications of intelligence value, the argument goes, any interception of Americans' communications is incidental. [redacted]"[22]

(U) The concept of "incidental interception" has a long history in cases that involve surveillance using "hard selection"—for example, surveillance under a wiretap.[23] In such cases, the "incidentally collected" communications had been sent to or from a specific person (or facility) targeted by the government.

(U) Two recent cases arising in the context of surveillance under Section 702 of the Foreign Intelligence Surveillance Act[24] illustrate the contours of this doctrine and its application outside of the "pure" wiretap context. In *United States v. Hasbajrami*,[25] the Second Circuit described "incidental collection" as occurring upon "the collection of the communications of individuals in the United States acquired in the course of the surveillance of individuals without ties to the United States and located abroad."[26] Such incidental collection, the Second Circuit held, "is permissible under the Fourth Amendment."[27] As an example, the Second Circuit observed that incidental collection could be premised on appropriate "targeting"—namely, "the

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

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

[23] (U) *See United States v. Kahn*, 415 U.S. 143 (1974); *Clay*, 430 F.2d at 170-72.

[24] (U) 50 U.S.C. § 1881a. The Second Circuit has recently, relying on a report of this Board, described section 702's statutory scheme. *See United States v. Hasbajrami*, 945 F.3d 641, 650-58 (2019) (citing PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014) ("PCLOB Section 702 Report")).

[25] (U) 945 F.3d 641 (2d Cir. 2019).

[26] (U) *Id.* at 646; *see id.* at 654 ("Incidental collection occurs when a non-targeted individual (a United States person or someone in the United States) communicates with a targeted non-United States person located abroad.").

[27] (U) *Id.* at 646. The Second Circuit distinguished such "incidental collection" from "inadvertent collection," which it defined as collection that

> occurs when the NSA reasonably believes that it is targeting a non-United States person located abroad, or does not have enough information to determine whether an individual e-mail address or other communications facility is being used by a United States person or accessed from within the United States, and therefore presumes that the account is controlled by a foreigner outside the United States. The collection is characterized as "inadvertent" when the agency learns that the person controlling the account is a United States person after it has already acquired some of the person's communications. In essence, inadvertent collection occurs when the NSA targets United States persons or individuals located within the United States in error: the agency thought it was targeting a foreign individual abroad, but the targeted person was in fact a United States person or an individual located in the United States.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

decision to surveil an individual or his or her channels of electronic communications"[28]—that comports with the Fourth Amendment.[29] And the Second Circuit reasoned that surveillance could be incidental, and permissible, even where the government expected that it would collect some United States person communications.[30] As the Second Circuit put it, "That the overall practice of surveilling foreigners abroad of interest to the legitimate purpose of gathering foreign intelligence information may predictably lead to the interception of communications with United States persons no more invalidates that practice, or requires the government to cease its surveillance of the target until a warrant is obtained, than the general foreseeability of intercepting communications with previously unknown co-conspirators undermines the inadvertent overhear doctrine in ordinary domestic criminal wiretapping."[31]

(U) In *United States v. Mohamud*,[32] the Ninth Circuit held that collection of the communications of a U.S. person who communicated with a foreign target "d[id] not require a warrant, because the search was targeted at a non-U.S. person with no Fourth Amendment right."[33] The court referred to this as the "incidental overhear" approach, borrowing from the familiar notion that, in the context of a traditional wiretap, "failure to identify every individual who could be expected to be overheard" does not make the acquisition unlawful.[34] The court also quoted this Board's description of incidental collection from the Board's 2014 report on Section 702, which also presumed a target: "The collection of communications *to and from a target* inevitably returns communications in which non-targets are on the other end, some of whom will be U.S. persons."[35]

(~~TS//SI//REL~~) The question presented by XKEYSCORE is whether the same concept of "incidental" collection applies where [redacted][36] In this respect, Section 702 surveillance arguably might be understood to bear greater resemblance to the

Id. at 656. Inadvertent collection, the Second Circuit said, "raises novel constitutional questions." *Id.* at 646.

[28] (U) *Id.* at 652. Targeting has a technical meaning in the context of FISA. In this Statement, my concern is "with the procedures designed to protect the constitutional privacy rights of Americans and comply with the Fourth Amendment inside the United States and not with the obviously confidential procedures and criteria by which United States intelligence agencies decide which non-United States persons located abroad are appropriate objects of surveillance." *Id.*

[29] (U) *Id.* at 664.

[30] (U) *Id.* at 665.

[31] (U) *Id.* As the Second Circuit observed, "[i]n the nature of law enforcement, there is always a possibility that the collection of evidence against a person who there is already probable cause to believe is involved in criminal activity or who is otherwise legitimately subject to surveillance will also develop information about others not previously reasonably suspected of wrongdoing." *Id.* The Second Circuit also observed that there was "no contention" that the surveillance "was undertaken as a pretext to collect the communications" of a U.S. person. *Id.*

[32] (U) 843 F.3d 420 (9th Cir. 2016).

[33] (U) *Id.* at 439.

[34] (U) *Id.* at 439 (quoting *United States v. Donovan*, 429 U.S. 413, 436 n.24 (1977)).

[35] (U) *Id.* at 440 (quoting PCLOB Section 702 Report at 82).

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

(b)(1)
(b)(3)-P.L. 86-36
(b)(5)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

familiar wiretap [redacted]. Section 702 has specific targets whose communications are intentionally collected, and various co-communicants whose communications are incidentally collected.[37] [redacted][38] The ingestion of some U.S.-person communications into XKEYSCORE may not be specifically intended, but it is a natural result of NSA's approach.

(U) Several considerations suggest that the incidental overhear concept applies under these circumstances, and counsels against the Fourth Amendment requiring further "targeting." First, as a conceptual matter, "[t]he 'incidental overhear' doctrine is closely related to the 'plain view' doctrine applied in connection with physical searches."[39] The "plain view" doctrine is applicable without further "targeting."[40] One might argue that, *a fortiorari*, the incidental overhear concept also does not require targeting.

(U) Second, several cases have made a comparable suggestion. In *Hasbajrami*, for example, Judge Lynch observed on behalf of the Second Circuit that

> law enforcement officers do not need to seek an *additional* warrant or probable cause determination to continue surveillance when, in the course of executing a warrant *or engaging in other lawful search activities*, they come upon evidence of other criminal activity outside the scope of the warrant or the rationale justifying the search, or the participation of individuals not the subject of that initial warrant or search.[41]

[redacted]

[37] (U) To be sure, until April 2017, NSA also used Section 702 to collect messages *about* targeted selectors, where "[a] U.S. person sen[t] or receive[d] an Internet communication that [was] routed internationally and that include[d] a reference to a selector such as an email address used by a foreigner who ha[d] been targeted." PCLOB Section 702 Report at 87; *see also id.* at 37-39.

[38] (~~TS//SI//REL~~) [redacted]

[39] (U) *Hasbajrami*, 945 F.3d at 664 n.17 (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 456-67 (1971)).

[40] (U) *See Coolidge*, 403 U.S. at 467-70.

[41] (U) 945 F.3d at 662 (some emphasis added). The Second Circuit repeatedly adopted this formulation, strongly suggesting it was a deliberate choice. *See id.* at 663 ("The Fourth Amendment generally is not violated when law enforcement officers, having lawfully undertaken electronic surveillance, whether under the authority of a warrant *or an exception to the warrant requirement*, discover and seize either evidence of criminal activity that they would not have had probable cause to search for in the first place, or the relevant conversation of an individual they did not

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

(b)(1)
(b)(3)-P.L. 86-36

(U) Judge Lynch's use of the clause referring to "engaging in other lawful search activities" suggests that the "incidental collection" concept applies whenever the government conducts a lawful search, not merely when it obtains a warrant. Thus, in *Hasbajrami* itself, the Second Circuit rejected the argument that the "incidental overhear" line of cases applied solely where "there was already an initial warrant supported by probable cause."[42] The Second Circuit held that "once that initial surveillance is rendered lawful by a warrant, a FISC order, *or some other exception to the warrant requirement*, an additional warrant is not necessary in order to collect the calls or e-mails of third parties."[43] "The reason why the initial surveillance was lawful," the Second Circuit continued, "does not matter to this conclusion."[44]

(U) Likewise, in *Mohamud*, the Ninth Circuit acknowledged that the leading precedents involving application of the "incidental overhear" doctrine involved searches that "targeted United States citizens and took place within the United States, so a warrant was required for the initial search to be constitutionally permissible."[45] The Ninth Circuit held that

> the guiding principle behind [the incidental overhear cases] applies with equal force here: when surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful.[46]

(U) The FISCR reached a similar conclusion in *In re Certified Question of Law*,[47] holding that incidental collection could be "constitutionally reasonable, even when done without a probable-cause warrant."[48] In that case, the government's use of a pen register—subject to a pen register application with a selection term,[49] but without probable cause or a warrant—collected, not merely metadata from a target's phone calls, but also "post-cut-through digits" dialed after a

---

anticipate or name in a warrant application.") (emphasis added); *id.* at 667 ("[W]hen an officer executing a lawful search or electronic surveillance warrant, *or otherwise engaged in a lawful search*, comes upon evidence of a previously unsuspected crime, or learns of the involvement of a previously unsuspected individual, the officer is not required to stop and obtain a new warrant to seize the item or to continue monitoring the phone line for which the warrant was obtained.") (emphasis added).

[42] (U) *Id.* at 665.

[43] (U) *Id.* at 665-66 (emphasis added).

[44] (U) *Id.* at 666.

[45] (U) 843 F.3d at 440.

[46] (U) *Id.* at 440-41 (citation and quotation marks omitted) (quoting *United States v. Hasbajrami*, 11-CR-623 (JG), 2016 WL 1029500, at *9 (E.D.N.Y. Mar. 8, 2016)). For similar language from the FISCR, see *In re Directives* 551 F.3d at 1015 ("It is settled beyond peradventure that incidental collections occurring as a result of *constitutionally permissible acquisitions* do not render those acquisitions unlawful. The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.") (emphasis added).

[47] (U) 858 F.3d 591 (FISA Ct. Rev. 2016).

[48] (U) *Id.* at 605.

[49] (U) *See* 50 U.S.C. § 1842(c)(3).

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

call was connected, which the Court classified as "content" information for purposes of the Fourth Amendment. The FISCR held that the collection of the post-cut-through digits was incidental to the collection of the metadata and, hence, constitutionally permissible. In doing so, the FISCR necessarily reasoned that the constitutionality of incidental collection does not hinge on the existence of a warrant supported by probable cause.[50]

(U) And the FISC has also reasoned similarly in a 2011 opinion by Judge Bates.[51] In that opinion, the FISC observed that it was addressing a factual scenario somewhat different from the standard "incidental collection" paradigm. It observed that, in the scenario before it, "the incidental acquisitions of concern are not direct communications between a non-target third party and the user of the targeted facility," nor "are they the communications of non-targets that refer directly to a targeted selector."[52] Instead, the issue at hand before the FISC concerned communications "acquired simply because they appear somewhere in the same *transaction* as a separate communication that is to, from, or about the targeted facility."[53] The FISC observed that "[t]he distinction is significant and impacts the Fourth Amendment balancing."[54] Ultimately, the FISC treated this "distinction" as a factor relevant to the balancing approach applied under the Fourth Amendment's Reasonableness Clause.[55]

~~(TS//SI//REL)~~

[redacted]

[50] ~~(TS//SI//REL)~~ [redacted]

See also Hasbajrami, 945 F.3d at 654 (discussing incidental versus inadvertent collection).

[51] (U) [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011) ("*2011 Bates Opinion*").

[52] (U) *2011 Bates Opinion* at *27.

[53] (U) *Id.* As the FISC observed, the NSA acquired the transaction "because it lack[ed] the technical means to limit collection only to the discrete portion or portions . . . that contain a reference to the targeted selector." *Id.* at *26.

[54] (U) *2011 Bates Opinion* at *27. Specifically, the FISC observed that "[a] discrete communication as to which the user of the targeted facility is a party or in which the targeted facility is mentioned is much more likely to contain foreign intelligence information than is a separate communication that is acquired simply because it happens to be within the same transaction as a communication involving a targeted facility." *Id.*

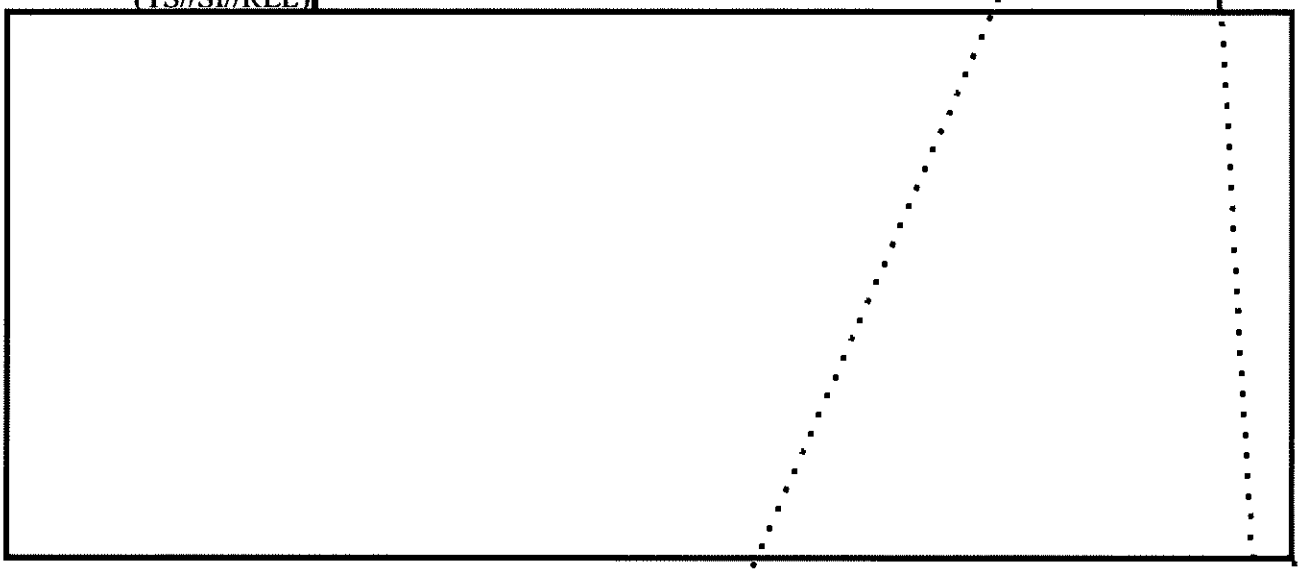
[55] (U) *2011 Bates Opinion* at *27-28.

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

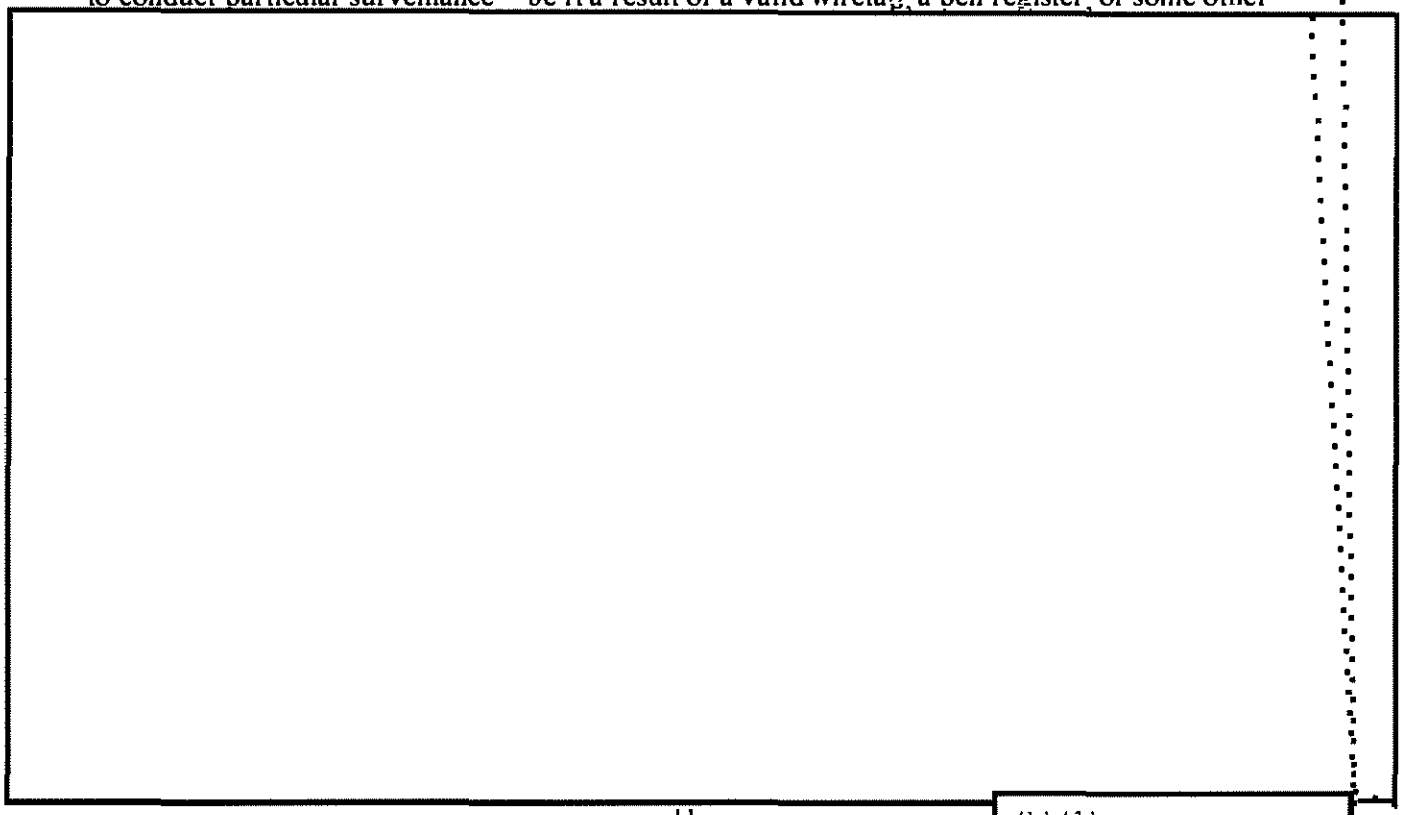
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(~~TS//SI//REL~~)



(~~TS//SI//REL~~) For the reasons given above, I believe that the principle of "incidental" collection applies in the context of XKEYSCORE. First, as a conceptual matter, it is most plausible to consider "incidental collection" or "incidental overhear" as an outgrowth of the "plain view" doctrine. When the government has the authority to conduct particular surveillance—be it a result of a valid wiretap, a pen register, or some other



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

aspect of the Fourth Amendment—collection of other, non-targeted persons may occur in the normal course as a matter of plain view. Second, as Judge Bates reasoned in his opinion for the FISC, the concept of "inadvertent" collection has important ramifications for the Fourth Amendment calculus, but those consequences seem best addressed in the analysis of a program's reasonableness, rather than by denying application of the incidental collection doctrine altogether. Indeed, Judge Lynch's discussion of "inadvertent collection" in *Hasbajrami* can be read to be consistent with this perspective.[62] Thus, though the issue is a challenging one with which various jurists have grappled in recent years, the better view is that the incidental collection doctrine is applicable in this context.

B.

(~~TS//SI//REL~~) Assuming that the "incidental collection" concept applies under these circumstances, such collection must fall within the ambit of, or be "incidental" to, the collection of some communications pursuant to an exception to the Warrant Clause of the Fourth Amendment. There appear to be two possible exceptions—the extraterritorial exception and the foreign intelligence exception—that might be applicable to the type of collection at issue here. I address the two in turn. The application of either one of these two exceptions would mean that the collection and analysis at issue in XKEYSCORE would remain subject to the Reasonableness Clause.

(b)(3)-P.L. 86-36
(b)(5)

1.

(~~TS//SI//NF~~) *Extraterritoriality.* I have already discussed the extraterritorial exception to the Fourth Amendment addressed in *Verdugo-Urquidez*, which applies to an overseas search of a non-U.S. person.[63] As I explained, *Verdugo-Urquidez* did not address the appropriate analysis when an overseas search of a non-U.S. person results in incidental collection of U.S.-person communications. Since the Court's decision in *Verdugo-Urquidez*, several courts have addressed that factual scenario, holding that the Warrant Clause does not apply extraterritorially to the searches of U.S. persons, but that the Reasonableness Clause does.[64]

[65]

[redacted]

[62] (U) In this respect, an analogy can be drawn between "inadvertent collection" and the "apparent authority" doctrine of Fourth Amendment law, which assesses for Fourth Amendment reasonableness government actions reasonably taken on information that later proved incorrect. *See* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 309 (2015) (citing *Illinois v. Rodriguez*, 497 U.S. 177, 179-80 (1990), and reasoning that "[t]he analogy between apparent authority and unknown *Verdugo-Urquidez* status should be clear").

[63] (U) *See supra* Part II.

[64] (U) In addition to the cases discussed in the text, see *United States v. Barona*, 56 F.3d 1087, 1094-95 (9th Cir. 1995), and *United States v. Peterson*, 812 F.2d 486, 490 (9th Cir. 1987). In both cases, the court determined that when American officials partner with foreign law enforcement officers in a "joint venture" to conduct a search of an American, the search must be reasonable under the Fourth Amendment. The opinions did not expressly address the warrant requirement, but neither required the government to obtain a U.S warrant for such a search.

[65] (U) A 1976 district court decision, *Berlin Democratic Club v. Rumsfeld*, held that prior judicial authorization by a U.S. magistrate *was* required, but in a very unusual situation. 410 F. Supp. 144 (D.D.C. 1976). That case involved a provision of West Germany's G-10 law, which governs telecommunications intercepts, that allowed U.S. officials to request that the West German government conduct wiretaps where necessary to protect occupying NATO forces.

(U) In *In re Terrorist Bombings of U.S. Embassies in East Africa*, the Second Circuit addressed how the Fourth Amendment applies to telephone wiretaps and physical searches targeting a U.S. citizen residing in Kenya.[66] The court held that "the Fourth Amendment's Warrant Clause has no extraterritorial application"; instead, "foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment's requirement of reasonableness."[67] Judge Cabranes's opinion explained that the Court had found no historical evidence in support of requiring U.S. warrants to conduct an overseas search and quoted the Supreme Court's statement in *Verdugo Urquidez* that "[w]hat we know of the history of the drafting of the Fourth Amendment . . . suggests that its purpose was to restrict searches and seizures which might be conducted by the United States in domestic matters."[68]

(U) In *United States v. Stokes*,[69] the Seventh Circuit considered a Fourth Amendment challenge to the use of evidence found in a raid, conducted jointly by U.S. government and Thai authorities, of an American citizen's residence in Thailand.[70] The Seventh Circuit adopted Judge Cabranes's reasoning and held that "the Fourth Amendment's warrant requirement, and by extension the strictures of the Warrant Clause, do not apply to extraterritorial searches by U.S. agents."[71] Instead, "the search of Stokes's home in Thailand [was] governed by the Amendment's basic requirement of reasonableness."[72]

(U) Recent court of appeals cases decided in the context of Section 702 have squarely held that the target's location and status, rather than the collection device's location, is controlling for application of the extraterritorial exception for Fourth Amendment purposes. That approach seems consistent with Chief Justice Rehnquist's view in *Verdugo-Urquidez* that the "available historical data show . . . that the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was never suggested that the provision was intended to restrain the actions of the Federal Government

---

The court held that the warrant requirement applied to a U.S. Army request to surveil U.S. citizens who were effectively domestic political activists, even though they were located overseas. That case, even assuming that it was correctly decided, is best seen as *sui generis*, in view of two unusual features. First, the surveillance, though conducted abroad, targeted activities by U.S. citizens that related to inherently domestic political issues. Second, the United States wielded quasi-sovereign authority in Berlin during the decades-long Allied occupation of that city—authority reflected in the unusual provision of the G-10 law.

(U) In *Best v. United States*, 184 F.2d 131 (1st Cir. 1950), the First Circuit held that a warrant was not required for a search conducted by the military "in the early months of the military occupation of Austria." *Id.* at 139. However, it suggested in *dicta* that a warrant would be required for FBI agents investigating a federal crime to search the dwelling in Germany of a U.S. citizen working in a civilian capacity for the U.S. government. *Id.* at 138.

[66] (U) 552 F.3d 157 (2d Cir. 2008).

[67] (U) *Id.* at 171.

[68] (U) *Id.* at 169 (quoting 494 U.S. at 266 (alterations in original)).

[69] (U) 726 F.3d 880 (7th Cir. 2013).

[70] (U) *Id.* at 885-86. *Stokes* involved a U.S. citizen, residing in Thailand, who was suspected of sexually exploiting children. *Id.* The U.S. and Thai governments conducted a joint raid of the defendant's home pursuant to a Thai search warrant, which uncovered voluminous evidence of his guilt. *Id.* at 886.

[71] (U) *Id.* at 893. The defendant had argued that the Thai warrant failed the Fourth Amendment's requirement of particularity and that "the search exceeded the scope of the warrant." *Id.* at 891.

[72] (U) *Id.* at 893.

against aliens outside of the United States territory."[73] The Second Circuit in *Hasbajrami* held that "a person who does not have a Fourth Amendment-protected privacy interest in his communications, such as a foreign national resident abroad, does not acquire such an interest by reason of the physical location of the intercepting device."[74] The Ninth Circuit in *Mohamud* reasoned that "what matters here is the location of the *target*, and not where the government literally obtained the electronic data."[75]

(U) Although this theory has yet to be expressly adopted by the Supreme Court, at least as the law currently stands, the implications from Chief Justice Rehnquist's opinion in *Verdugo-Urquidez* and the holdings in *Hasbajrami* and *Mohamud* indicate that the application of the extraterritorial exception depends on the nature of the communications intercepted, as opposed to the location of the intercepting device. The Fourth Amendment's backstop requirement of reasonableness still applies.

2.

(U) *Foreign intelligence.* The Supreme Court has left open the possibility that the Fourth Amendment may require different "safeguards" in the national security context than in ordinary criminal cases.[76] Based on such language, lower courts, including the Foreign Intelligence Surveillance Court of Review, have embraced a "foreign intelligence" exception to the Fourth Amendment's warrant requirement.[77] These courts have held that foreign-intelligence searches must satisfy the Fourth Amendment requirement of reasonableness, rather than the usual requirement that the government obtain probable cause and a warrant.

(U) The Foreign Intelligence Surveillance Court of Review has explained current doctrine in the following manner:

[73] (U) 494 U.S. at 266.

[74] (U) 945 F.3d at 665; *id.* at 664 (rejecting the argument that "*Verdugo-Urquidez* does not control the outcome here because Section 702 collection occurs in the United States"). The Second Circuit explained that "*[a]t least where the communication is collected essentially in real time as it occurs*, the targeted communication . . . occurs in the relevant sense where the person whose calls or e-mails are being intercepted is located, regardless of the location of the means used to intercept it." *Id.* (emphasis added).

[75] ~~(TS//SI//NF)~~ *Mohamud*, 843 F.3d at 439 (quotation marks omitted) (quoting *Hasbajrami*, 2016 WL 1029500, at *9 n.15) (rejecting the defendant's argument that "under *Verdugo-Urquidez*, the location of the search matters, and that here, the searches took place in the United States"); *see also* DAVID KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 17:3 (2016) ("For non-U.S. person targets, there is no probable-cause requirement; the only thing that matters is . . . the government's reasonable belief about . . . the target's location."). Thus, with respect to the type of collection at issue in the XKEYSCORE context, the location of the device is not dispositive.

[redacted]

[76] (U) *Katz*, 389 U.S. at 358 n.23; *United States v. U.S. Dist. Court for E. Dist. of Mich.*, 407 U.S. 297, 308-09 & n.8 (1972).

[77] (U) *See In re Directives*, 551 F.3d at 1010; *Truong*, 629 F.2d at 915; *accord Butenko*, 494 F.2d at 605; *Brown*, 484 F.2d at 426.

> When law enforcement officials undertake a search to uncover evidence of criminal wrongdoing, the familiar requirement of a probable-cause warrant generally achieves an acceptable balance between the investigative needs of the government and the privacy interests of the people. But it has long been recognized that some searches occur in the service of "special needs, beyond the normal need for law enforcement," and that, when it comes to intrusions of this kind, the warrant requirement is sometimes a poor proxy for the textual command of reasonableness.
>
> . . .
>
> [I]n this context, the warrant requirement is ill-suited to gauge what is reasonable. The textual command of reasonableness—"the ultimate touchstone of the Fourth Amendment,"—still governs. Indeed, it retains its whole force.[78]

(b) (3)-P.L. 86-36
(b) (5)

(U) Although lower court cases have embraced a foreign-intelligence exception to the Warrant Clause, the precise contours of such an exception can be debated. [redacted][79] On another view, the foreign-intelligence exception to the Warrant Clause applies somewhat more broadly. As the FISCR has put it, the "warrant requirement . . . 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*" rather than investigating criminal wrongdoing.[80] Similarly, the Third and Fifth Circuits have suggested in *dicta* that the exception turns on the purpose of the government's action, and applies to activities whose *purpose* is "gathering foreign intelligence."[81]

(~~TS//SI//REL~~) [redacted] the ultimate question is whether the foreign-intelligence exception applies solely when government surveillance is "directed at a foreign power of agent of a foreign power" or whether it also applies when government surveillance is conducted for a foreign-intelligence *purpose*, rather than the purpose of investigating ordinary crime. The daylight between these two ways of formulating the standard may matter in the specific context of the collection analyzed by XKEYSCORE, because such collection is not necessarily "directed at a foreign power or agent of a foreign power." For example, the law at issue in *In re Directives* permitted warrantless collection targeting a *particular, known* non-U.S. person located overseas.[82] The uses of XKEYSCORE the Board has reviewed in the Report do not involve collecting the communications of a specific, targeted person. [redacted]

[78] (U) *In re Certified Question of Law*, 858 F.3d 591, 605, 607 (FISA Ct. Rev. 2016) (citations omitted) (first quoting *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995); and then quoting *Riley v. California*, 573 U.S. 373, 381 (2014)).

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

[80] (~~TS//SI//NF~~) *In re Certified Question of Law*, 858 F.3d at 593 (emphasis added); [redacted]

[81] (U) *Butenko*, 494 F.2d at 605; *Brown*, 484 F.2d at 426.

[82] (U) 551 F.3d at 1007.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]

(~~TS//SI//NF~~) That programmatic purpose is consistent with Executive Order 12,333, which does not limit the universe of information that can be collected by intelligence agencies to information about foreign powers or their agents.[83] Accordingly, NSA procedures permit officers to target non-U.S. persons who possess, or are likely to possess, "foreign intelligence information," whether or not they work for or on behalf of a foreign power.[84]

(~~TS//SI//NF~~) That programmatic purpose is also somewhat akin to the purpose behind the surveillance authorized under Section 702 of FISA. As the Supreme Court has observed, "[u]nlike traditional FISA surveillance, [Section 702] does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or [an] agent of a foreign power."[85] Instead, under Section 702, on "the issuance of an order" by the FISC, "the Attorney General and the Director of National Intelligence may authorize jointly . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[86]

(~~TS//SI//REL~~) It is possible that the narrower conception of the foreign-intelligence exception articulated in some precedents—which would limit foreign intelligence collection to foreign powers and their agents—is mere *dicta* not necessary to decide the case. [redacted][88]

(b) (3)-P.L. 86-36
(b) (5)

[83] (U) Executive Order No. 12,333 § 3.5(c).

[84] (U//~~FOUO~~) See USSID SP0018, as discussed in Part IV.B of the Board's Report.

[85] (U) *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 404 (2013).

[86] (U) 50 U.S.C. § 1881a(a). FISA defines "foreign intelligence information" in 50 U.S.C. § 1801(c).

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

[88] (U) *Id.* In *In re Directives*, the FISCR addressed a situation where the surveillance took place in the United States, but the target was located overseas. The FISCR formulated its holding in terms of those facts: "[W]e hold that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States." 551 F.3d at 1012.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

C.

(~~TS//SI//REL~~) Finally, assessing whether the collection and analysis that comprises XKEYSCORE complies with the Fourth Amendment will, if all collection is properly within or "incidental" to the extraterritorial or foreign intelligence exceptions, be assessed under the "the totality of the circumstances" test for reasonableness.[89] That "reasonableness" inquiry would depend in part on the "privacy protecting measures," such as restrictions on the targeting of U.S. persons and measures to minimize the retention and dissemination of information about U.S. persons in a manner consistent with mission need.[90]

(~~TS//SI//REL~~) Ultimately, this analysis likely turns on whether NSA adequately protects any U.S.-person communications processed by XKEYSCORE from misuse. The stronger the safeguards applicable to Americans' communications—such as limits on selection and retention and other protections for U.S. persons—the stronger the case for reasonableness. For example, significantly lengthening the retention periods, or [redacted] would likely raise the level of legal risk. [redacted] by contrast, would reduce such risk."[91] Without exhaustively addressing each aspect of the program here, to my mind, the protections enumerated in the Board's Report and highlighted in the separate statement of Chairman Klein

[89] (U) *Mohamud*, 843 F.3d at 441; *In re Terrorist Bombings*, 552 F.3d at 172 ("To determine whether a search is reasonable under the Fourth Amendment, we examine the totality of the circumstances to balance, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests.") (internal quotation marks omitted) (quoting *Samson v. California*, 547 U.S. 843, 848 (2006)). One question that can arise in litigation is whether the "reasonableness" of the program must be assessed at the time of the collection of information or whether the "reasonableness" of each individual search qualifies as a Fourth Amendment episode. Courts have split on this question. The district court in *Mohamud* concluded that the "subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment." *United States v. Mohamud*, No. 3:10-cr-475-KI-1, 2014 WL 2866749, at *26 (D. Or. June 24, 2014), *aff'd*, 843 F.3d 420, 440 n.24 (9th Cir. 2016) (explaining that the court was not resolving whether the "incidental overhear" concept permits the "retention and querying of the incidentally collected information"). The Second Circuit in *Hasbajrami*, however, concluded that "querying . . . stored data does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable." 945 F.3d at 670. Viewed from either the perspective of *Hasbajrami* or the district court in *Mohamud*, the lesson to be derived from these cases is that back-end privacy protections on storage and querying can affect the "reasonableness" of a program.

[90] (U) *Mohamud*, 843 F.3d at 443; *Hasbajrami*, 945 F.3d at 655 (describing FISA's minimization procedures).

[91] (~~TS//SI//NF~~) In considering the constitutionality of a government program that conducts many searches, the Supreme Court has analyzed the reasonableness of the entire program rather than of a particular search. *See Mich. Dep't of State Police v. Sitz*, 496 U.S. 444 (1990) (analyzing the reasonableness of Michigan's program of drunk driving checkpoints); *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656 (1989) (analyzing the reasonableness of the U.S. Customs Service's drug-testing program for employees seeking sensitive positions); *Skinner v. Ry. Labor Execs. Ass'n*, 489 U.S. 602 (1989) (analyzing the reasonableness of a drug-testing program for railway employees); *Bell v. Wolfish*, 441 U.S. 520 (1979) (analyzing the reasonableness of a prison's practice of conducting body-cavity searches of any inmate who had just met with a visitor). [redacted] do not aim to resolve that question here.

(b) (1)
(b) (3)-P.L. 86-36

indicate that the NSA has a strong case for XKEYSCORE's reasonableness on the present facts.[92]

(~~TS//SI//REL~~) If the program evolves, so too may the reasonableness analysis. Thus, keeping the Board (and, as appropriate, other oversight entities) apprised of "changes to XKEYSCORE that could materially affect the privacy or civil liberties of US persons," as we recommend in the accompanying Report, can help ensure sufficient scrutiny of changes that could affect the legal calculus.

* * *

(U) When President Truman established the NSA in 1952, he announced in a then-classified memorandum that the "COMINT mission of the National Security Agency (NSA) shall be to provide an effective unified organization and control of the communications intelligence activities of the United States conducted against foreign governments" and that the Nation's COMINT activities must "exploit to the maximum the available resources in all participating departments and agencies."[93] When the Fourth Amendment was written, ratified, and incorporated into the Constitution in the eighteenth century, its authors sought to prohibit the federal government from engaging in "unreasonable searches and seizures" and from obtaining warrants other than in certain specified circumstances. The passage of decades has not made the harmonization of these two directives any easier, nor has it rendered either directive any less vital. I have offered the preceding thoughts and analysis in an effort to ensure that the agency meets its obligations under both directives.

[92] (~~TS//SI//REL~~) To be sure, I do not arrive at a final conclusion on the Fourth Amendment reasonableness of the uses of XKEYSCORE addressed in the Board's Report. Such a conclusion would necessarily depend on a fact-intensive inquiry, including a review of the program's compliance record, which was not fully analyzed by the Board in its Report. Such a reasonableness analysis, thus, remains for the agency to conduct and for appropriate oversight entities (including the Board) to review in the future.

[93] (U) Memorandum to the Secretary of State and the Secretary of Defense from Harry S. Truman, President of the United States, *Communications Intelligence Activities* 1, 5 (Oct. 24, 1952).

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

(~~S//NF~~) Legal Analysis of XKEYSCORE
20 January 2016

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (5)

(U) 1. Executive Summary

~~(TS//SI//REL TO USA, FVEY~~ The President's Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board") is conducting a review of certain Intelligence Community counterterrorism operations conducted pursuant to Executive Order 12333, as amended (E.O. 12333). In connection with this review, by letter dated 15 December 2015, the PCLOB submitted a document request to the National Security Agency/Central Security Service ("NSA" or "Agency") seeking, among other things:

> **"Legal analysis by the NSA and the Department of Justice regarding the use of XKEYSCORE's analytic functions and its consistency with statute, executive order, and the Constitution."**

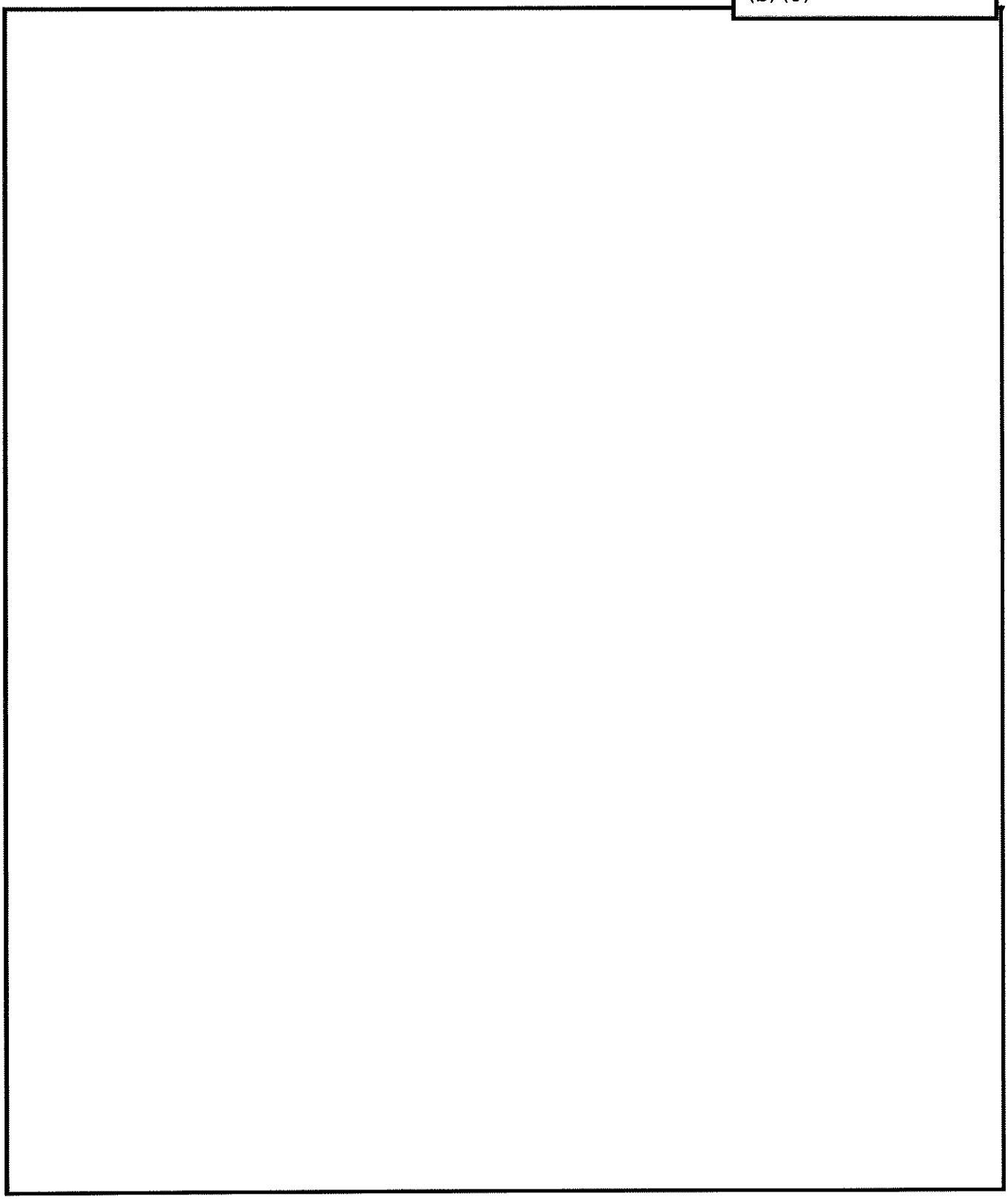
NSA's Office of General Counsel (OGC) prepared this paper in response to the Board's request. This paper is based on OGC's previous internal legal analyses.

(b) (3)-P.L. 86-36
(b) (5)

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

(U) II. Background

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



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

[redacted]

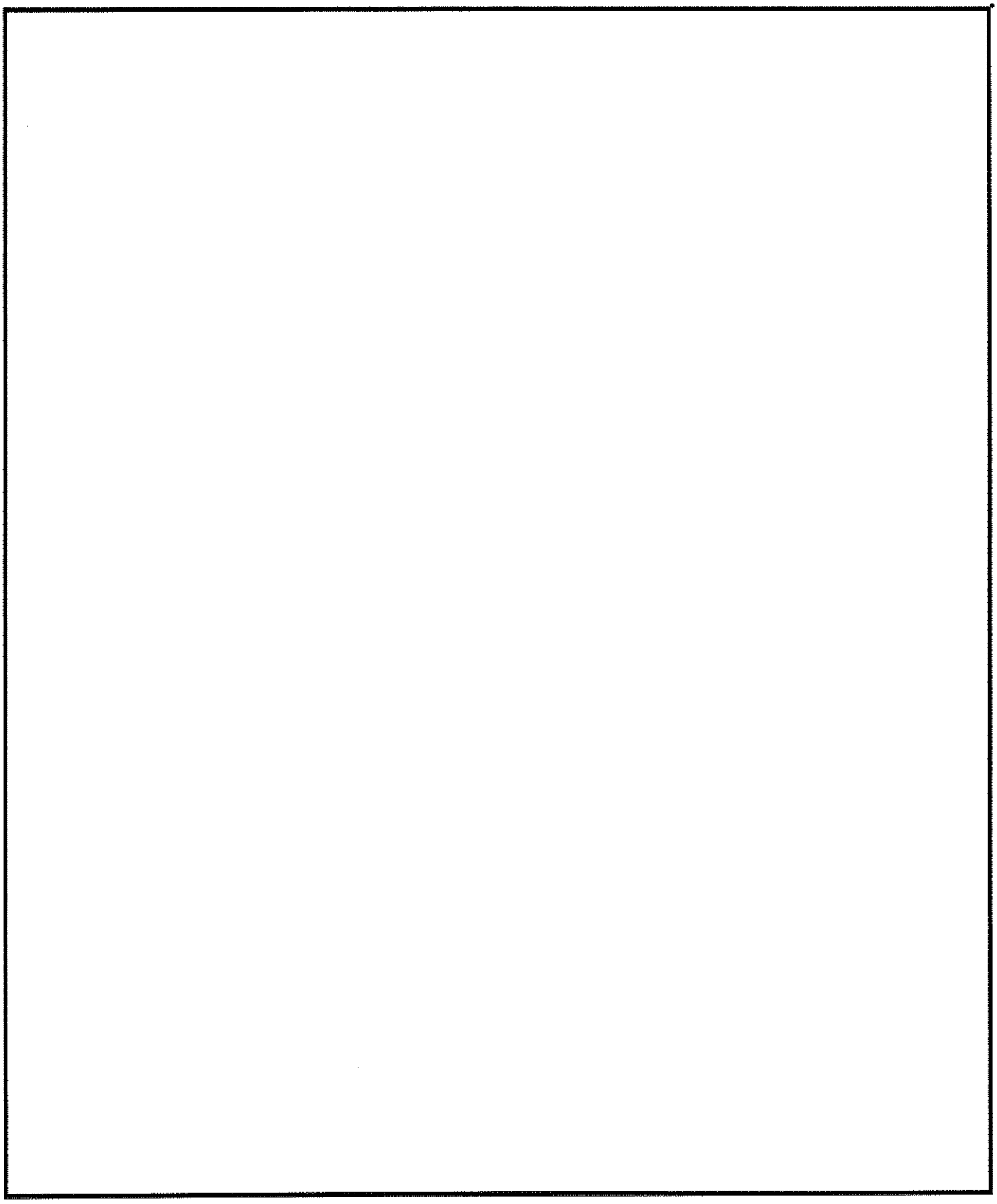
(U) III. Legal Analysis

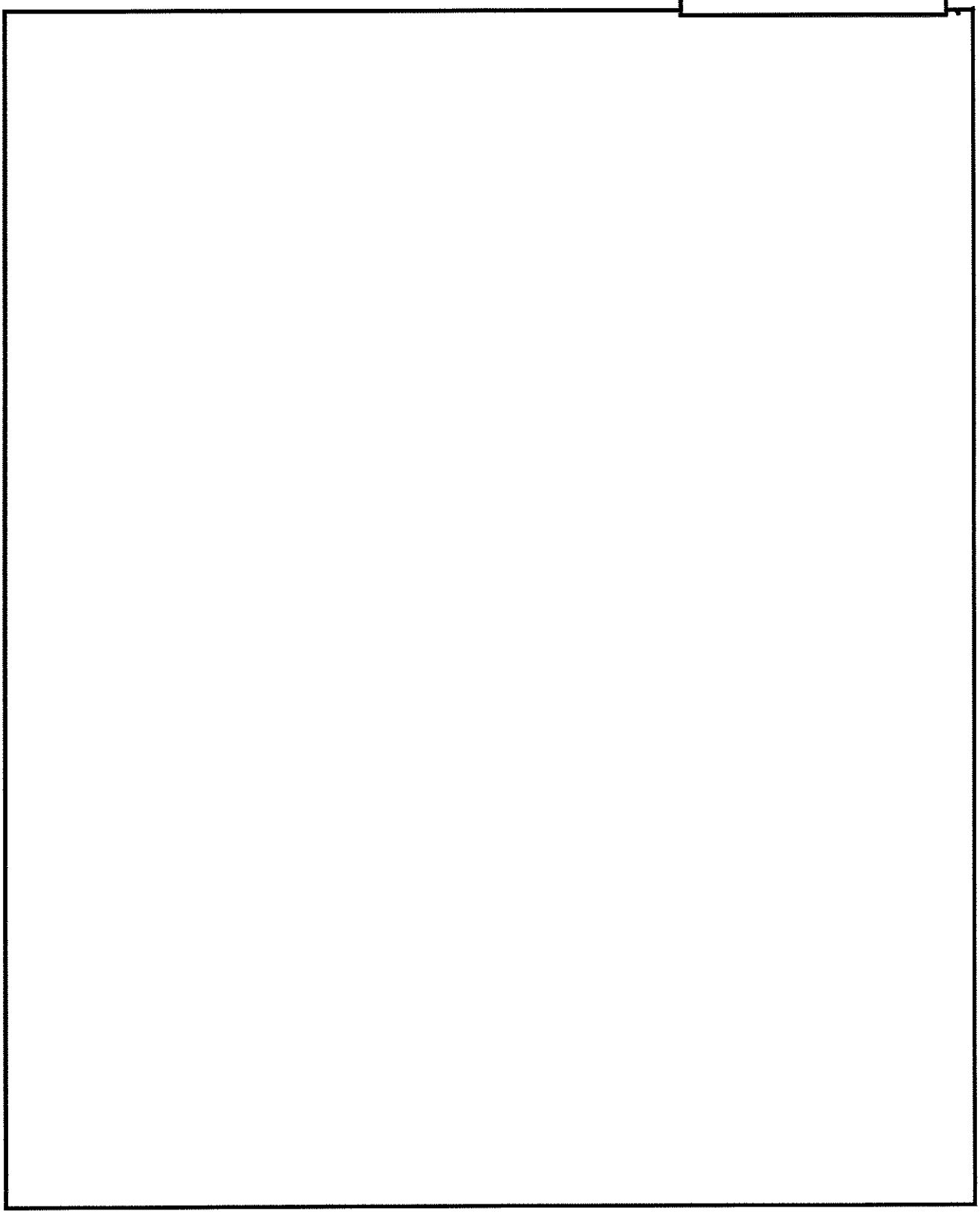
[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

(b) (3)-P.L. 86-36
(b) (5)

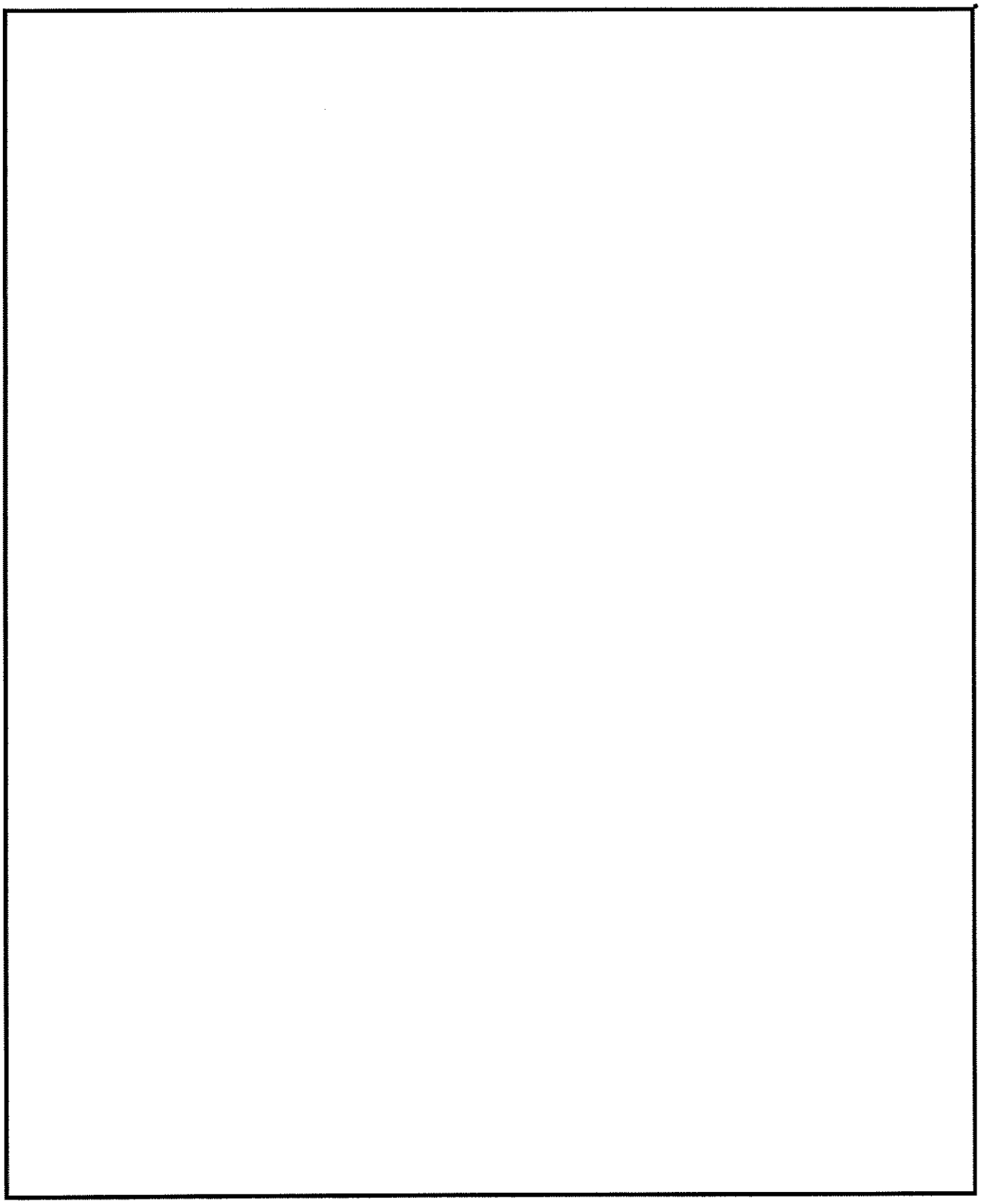
~~TOP SECRET//SI//NOFORN~~

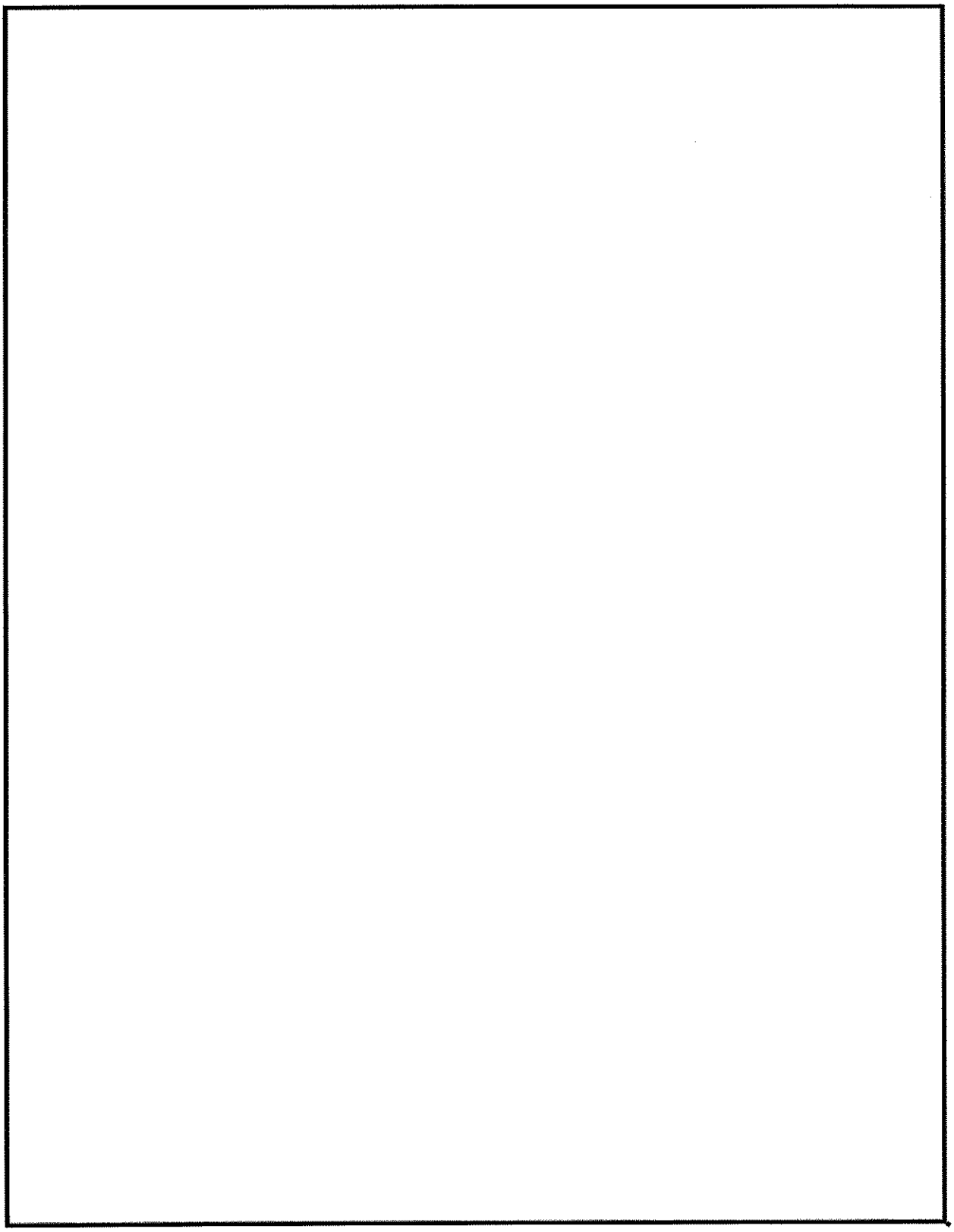




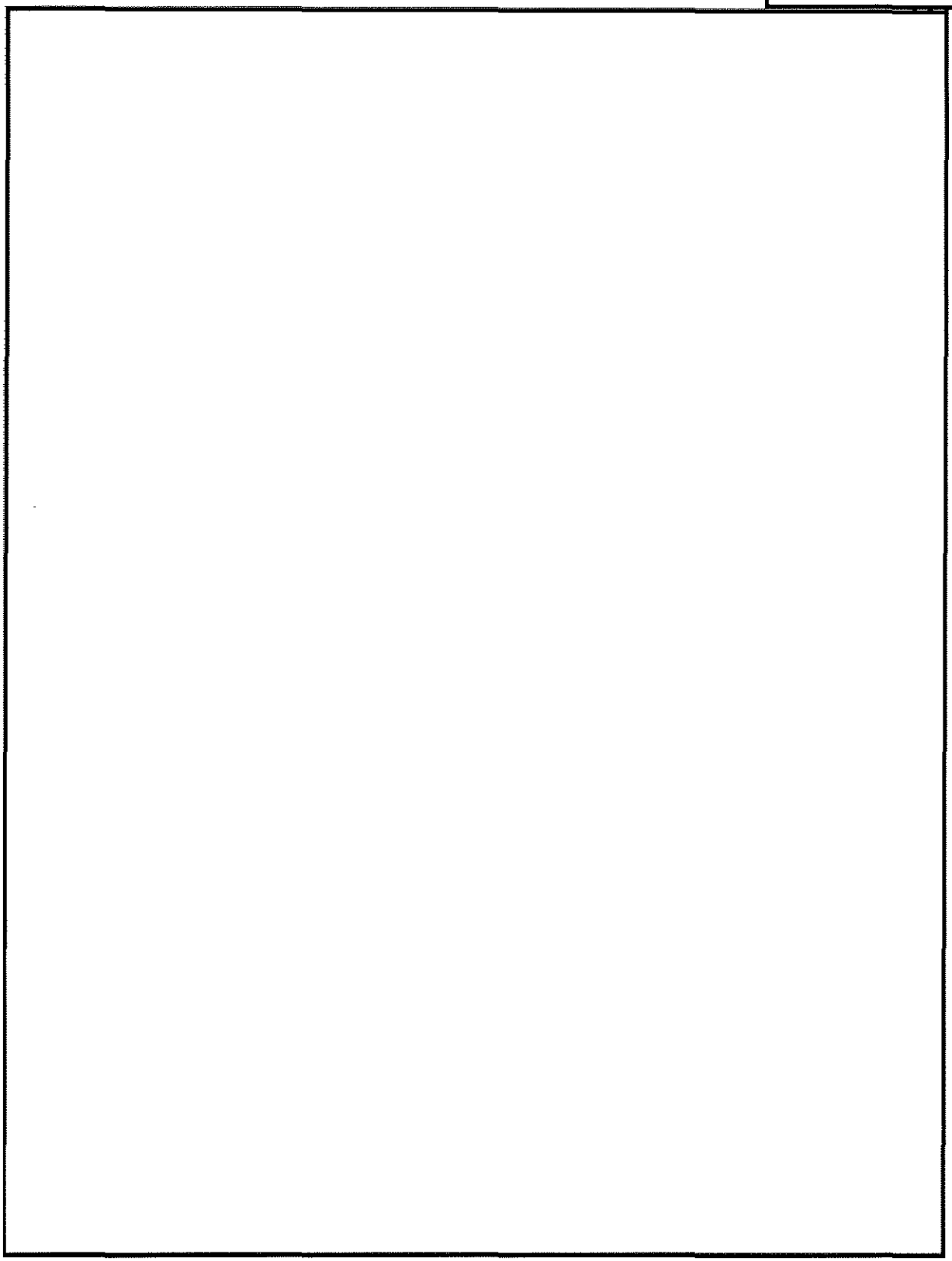
(b) (3)-P.L. 86-36
(b) (5)

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

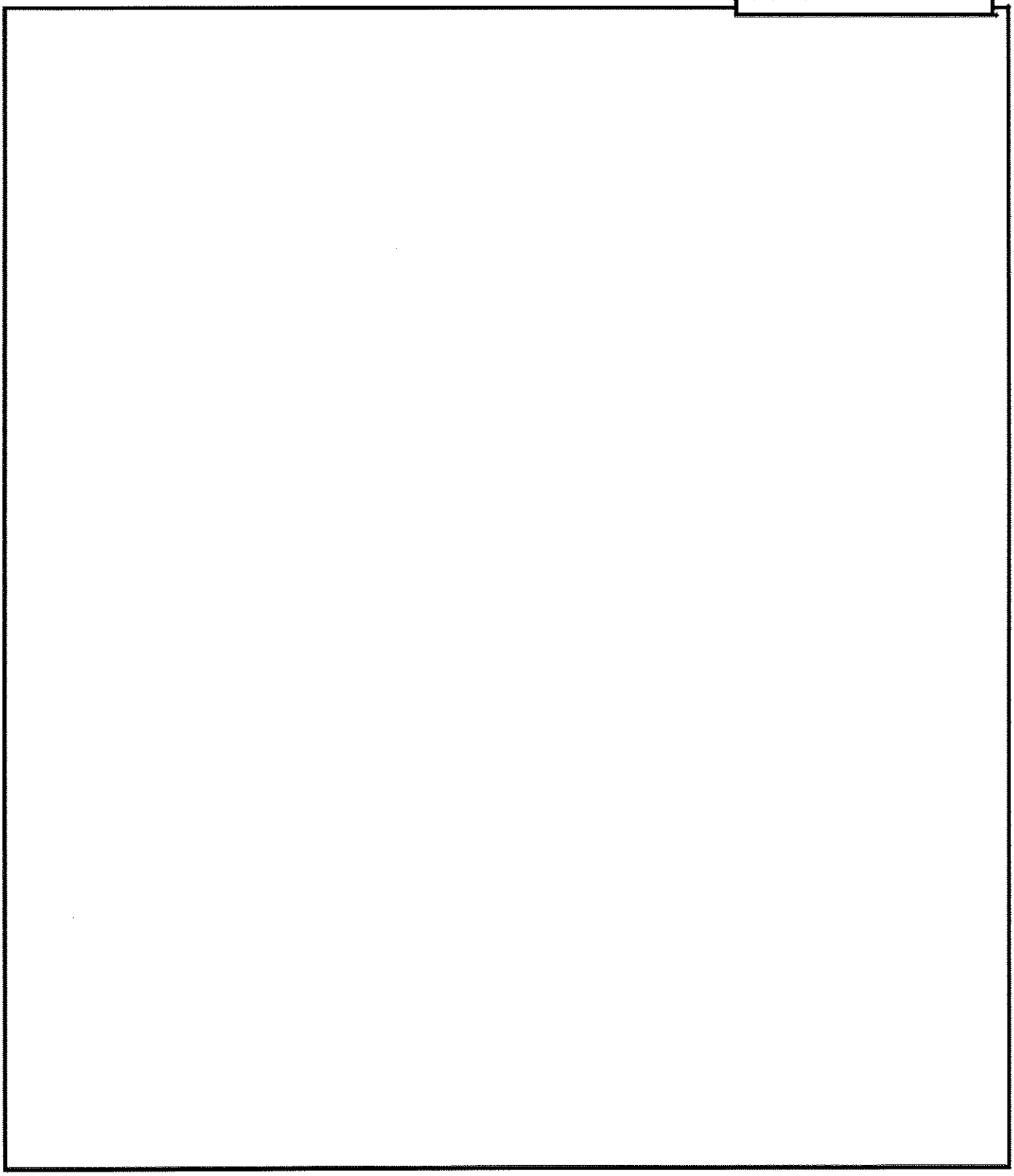


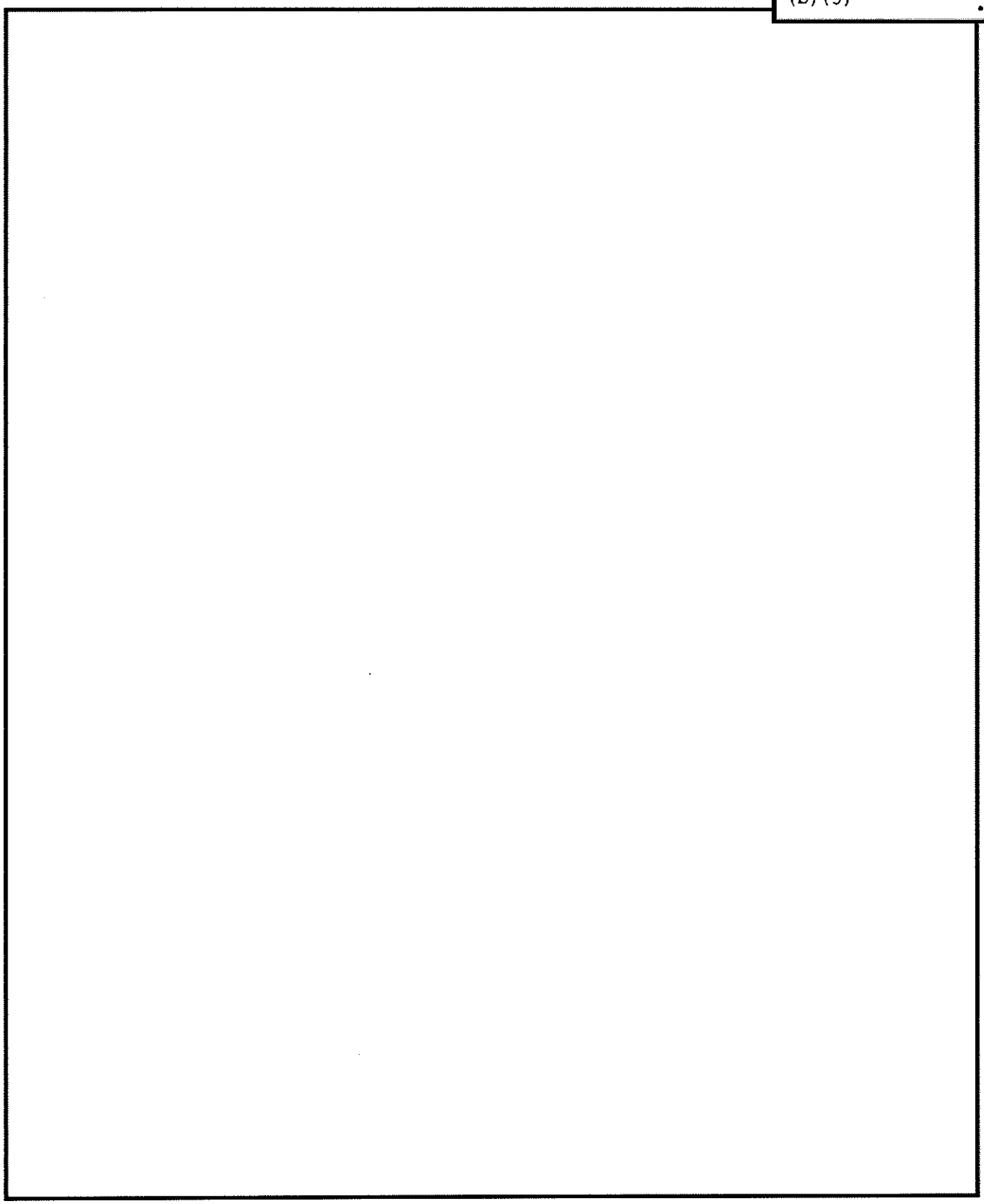


(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)



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





(b)(3)-P.L. 86-36
(b)(5)

[redacted]

(U) V. Conclusion

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(5)

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

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

PCLOB Questions received on September 14, 2020 regarding XKEYSCORE Deep Dive.

November 5, 2020

The answers are specific to how NSA uses XKEYSCORE under E.O. 12333

1. (~~TS//SI//NF~~) The Board would like a bit more information on collection.
   a.
      i. (~~TS//SI//NF~~) **NSA Response:**
   b.
      i. (~~TS//SI//NF~~) **NSA Response:**
   c.
      i. (~~TS//SI//NF~~) **NSA Response:**

2. (~~TS//SI//NF~~) The Board would like a bit more information on auditing.
   a. What are the protocols that are used to flag items to be reviewed by auditors?
      i. (U//~~FOUO~~) **NSA Response:** NSA is not entirely clear what is meant by flagging an item in this context. Every analyst query within XKEYSCORE is sent to the NSA corporate auditing tool for post query review. The queries are provided to the auditors and the auditors are required to evaluate the compliance of the query by the next business day. The auditor annotates the query record as "approved" or "reportable". Reportable queries are investigated as to whether a questionable intelligence activity has occurred. If yes, the incident report is included in

(b)(3)-P.L. 86-36

Classified By:
Derived From: NSA/CSSM 1-52
Dated: 20180110
Declassify On: ~~20450901~~

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

(b)(1)
(b)(3)-P.L. 86-36

the NSA Quarterly Report to the DoD Senior Intelligence Oversight Official (SIOO).

b. How many times have a query been flagged?
   i. (~~TS//SI//NF~~) **NSA Response:** (U//~~FOUO~~) During calendar year 2019, incident reports were submitted for XKEYSCORE database queries in; of those were identified as questionable intelligence activities (QIAs). See answer above.

c. Has a human auditor ever flagged a query?
(U//~~FOUO~~) **NSA Response:** To the extent flagging a query is meant to convey that an auditor had a concern with a query, there have been query compliance incidents by analysts in XKEYSCORE. See above figures for incident reports submitted and evaluated.

d. Can you confirm that there have been no previous incidents in XKEYSCORE?
(U//~~FOUO~~) **NSA Response:** As noted above, NSA has had incidents in XKEYSCORE. Compliance incidents occur during NSA mission activities, and NSA reports them immediately upon recognition and then compiles a quarterly report to overseers.

e. Are there any other statistics related to this kind of internal oversight?
(U//~~FOUO~~) **NSA Response:** The statistics related to the number of possible incidents and QIAs are the statistics NSA maintains and reports to DoD and ODNI. Post-query review is an NSA internal control. NSA has other internal controls to provide assurance of privacy protections during mission operations. These controls include data tagging, data access, query rules, targeting rules, purge, and data age-off.

3. (~~TS//SI//NF~~) The Board would like to know a bit more about the deprioritization system. Specifically, the Board wants to know what NSA does to deprioritize the viewing of US person traffic. We explained that you actually see it as a prioritization of foreign intelligence information and not a deprioritization of the viewing of US person traffic.

I know we discussed this a bit earlier this year, but even a few more facts will help us on this point.

a. (~~S//SI//REL~~) **NSA Response:** NSA focuses on positively identifying and promoting traffic likely to contain foreign intelligence

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

b. ~~(TS//SI//REL USA, FVEY)~~

a. ~~(TS//SI//REL USA, FVEY)~~

4. ~~(TS//SI//NF)~~ One Board member is interested in

a.

(U) **NSA Response:** It depends on a number of considerations, which are discussed in more detail below.

~~(TS//SI//REL USA, FVEY)~~

~~(TS//SI//REL USA, FVEY)~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~(TS//SI//REL USA, FVEY)~~

~~(TS//SI//REL USA, FVEY)~~

b.

(U)**NSA Response:** In many cases. See answer above.

c.

~~(TS//SI//REL USA, FVEY)~~ **NSA Response:**

5. ~~(TS//SI//NF)~~ USP Queries in XKS

a. Do we know the number of United States person queries (into XKS data) conducted each year since 2016?

~~(TS//SI//NF)~~ **NSA Response:** Analysts query USP within XKEYSCORE. As part of the query process, a justification including whether it is a USP query or not is required and follows the auditing process noted above. NSA has recently implemented an ability to track if the query is a USP. To that end, between January 2020 and September 2020, NSA identified USP queries.

b. We understand that these queries are only allowed for Is there a way to determine what the basis of these queries were?

~~(TS//SI//NF)~~ **NSA Response:** Currently, under NSA's Classified Annex procedures, are the only USP queries permitted in unevaluated EO 12333 SIGINT collection. Each query justification states the reason for the search. NSA would have to manually review all justifications since January 2020 and categorize them.

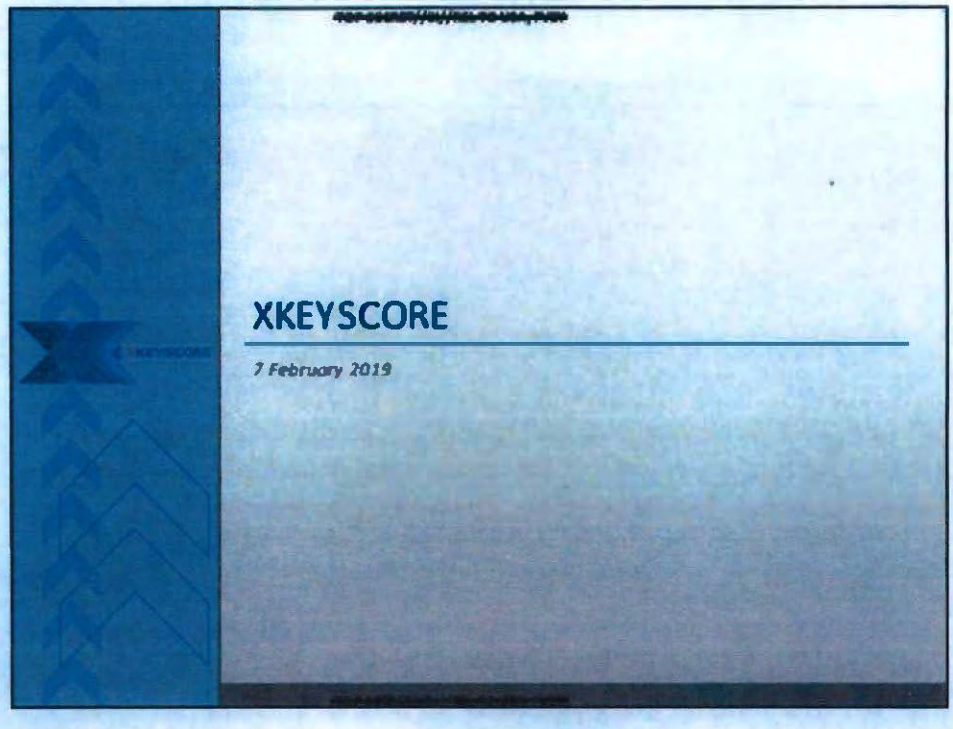
6. ~~(TS//SI//NF)~~ Data Processing:
   a. What kind of process is used to determine which data is processed by XKESYCORE?
   (U//~~FOUO~~) **NSA Response:** See response above regarding prioritization v. de-prioritization.

   b. Is that an automated system (collection)?
   (U//~~FOUO~~) **NSA Response:** See response above regarding prioritization v. de-prioritization.

   c. How is the process governed?
   (U//~~FOUO~~) **NSA Response:** See response above regarding prioritization v. de-prioritization.

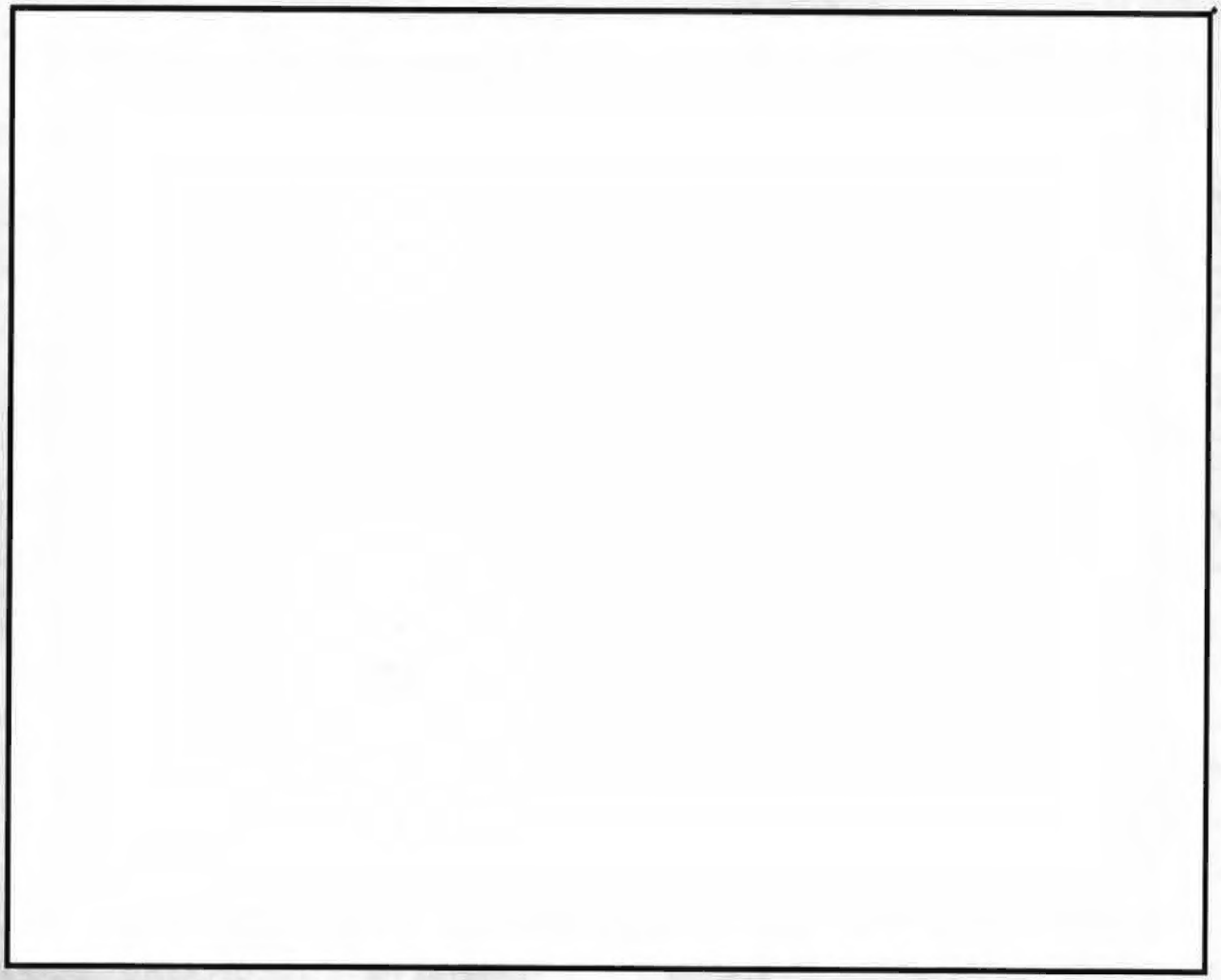
   d. Are privacy and civil liberties considered?
   (U) **NSA Response:** NSA is focused on identifying foreign intelligence. During the survey process, the assessment is on identifying foreign intelligence. It is not focused on privacy and civil liberties. Nevertheless, the outcome is that the focus on FI reduces the impact on USP privacy and civil liberties.

7. ~~(S//NF)~~ Is it true that XKEYSCORE training is voluntary (not mandatory)?
   ~~(S//NF)~~ **NSA Response:** Yes, XKS-specific training is voluntary, but there is mandatory training for access to any of the SIGINT as has been described previously. While the XKS tool training is not mandatory, the compliance training is compulsory. In fact, if any of the compliance trainings are not up-to-date, all access to XKEYSCORE is lost.

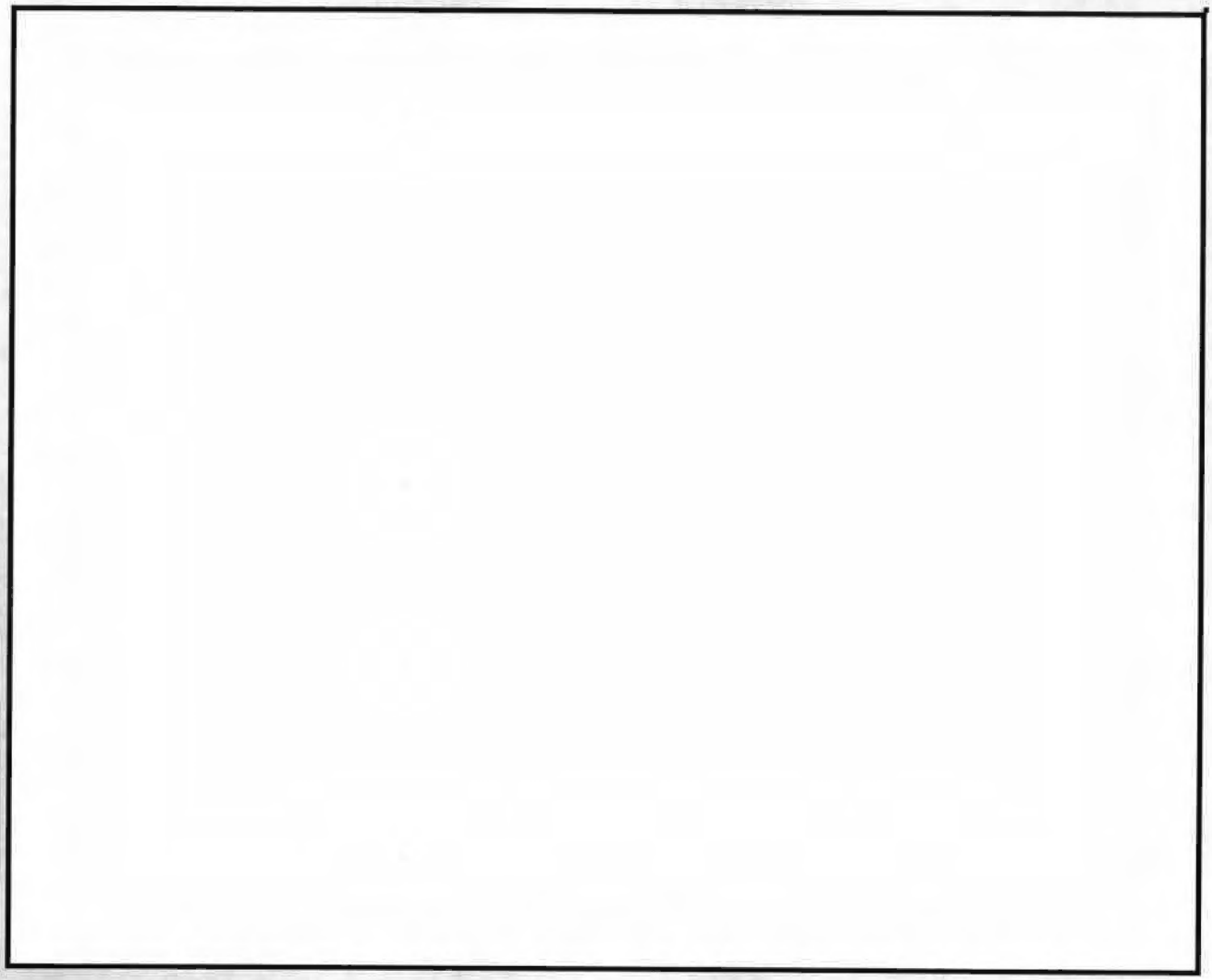


Hi I'm XKEYSCORE

(b)(3)-P.L. 86-36

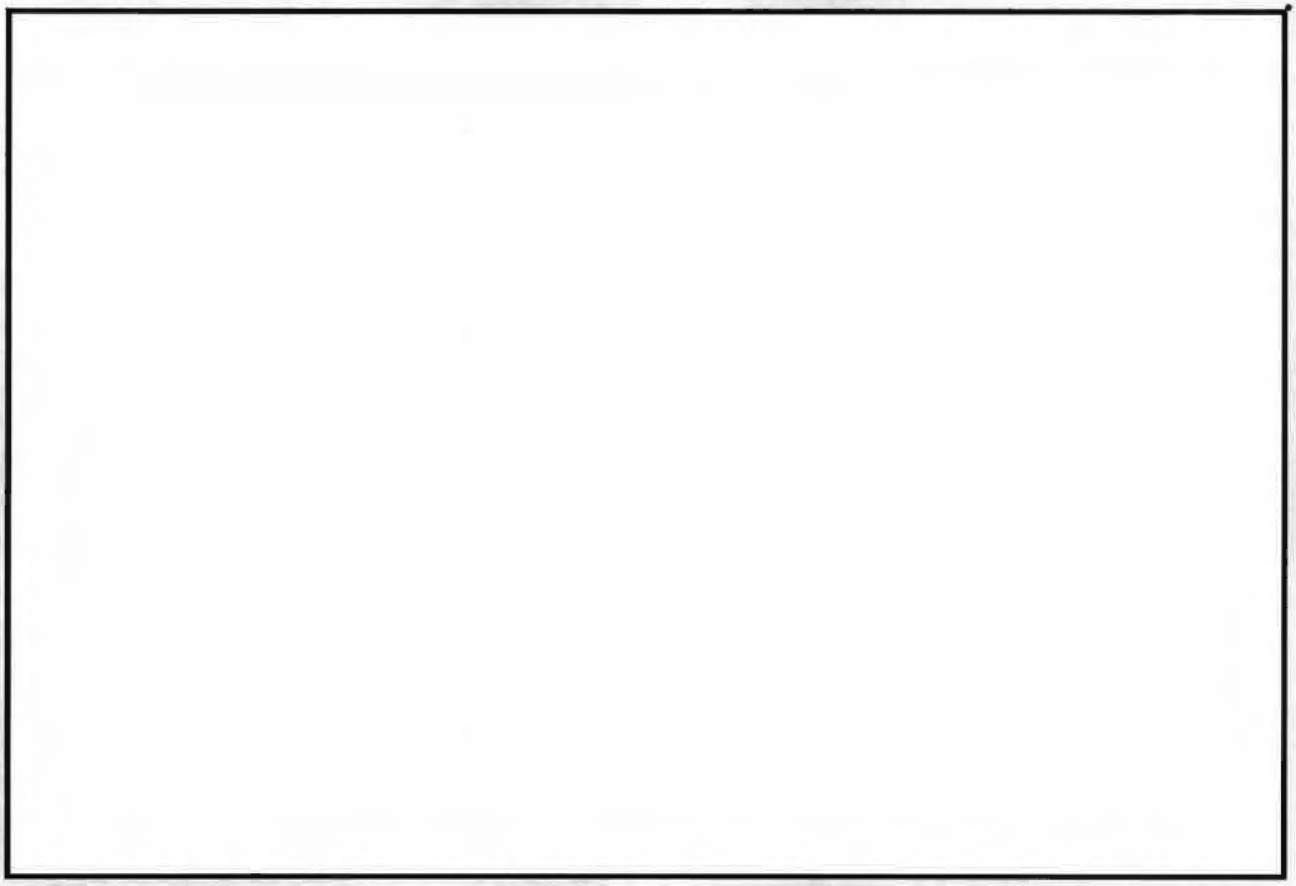


(b) (3)-P.L. 86-36

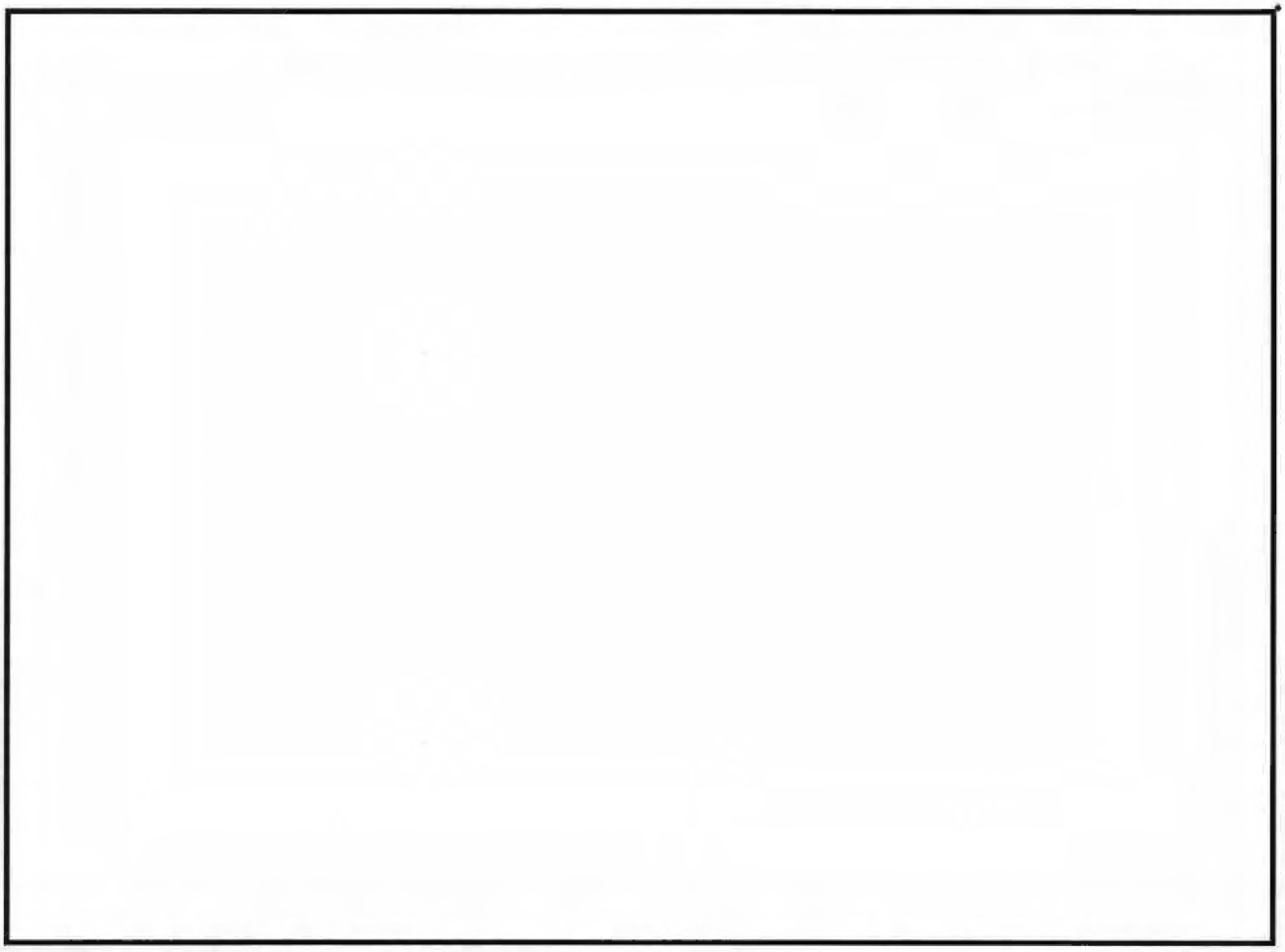


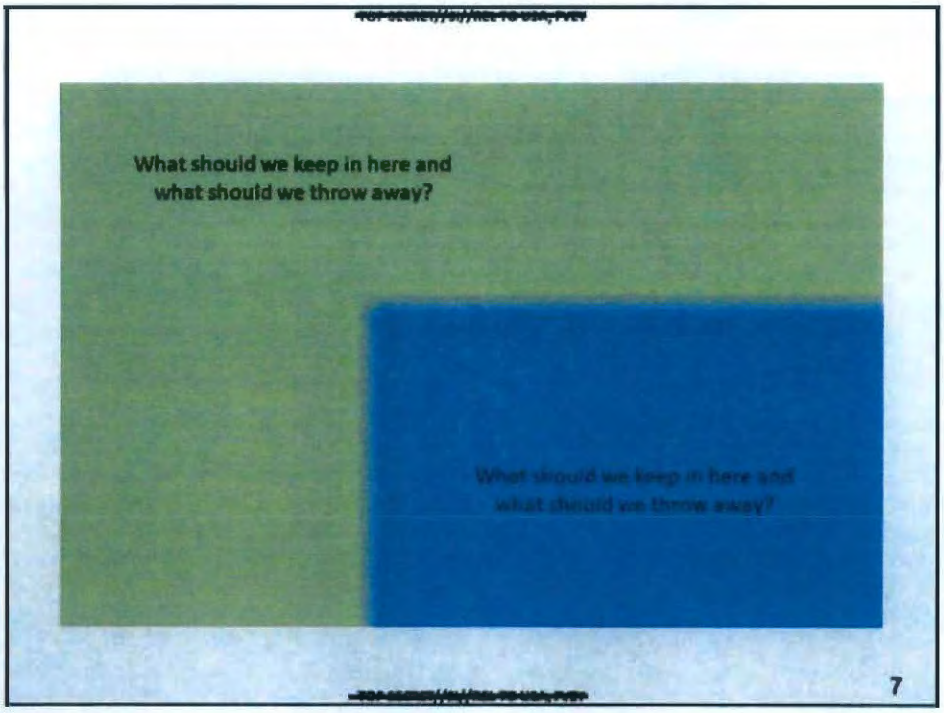
Once we have made that decision, we have to decide which signals are worth processing. It's very much like an old-fashioned manual phone switch. Some signals will get processed and some won't. Only the ones that are determined to have the most foreign intelligence value in accordance with USSID 18 will be processed.

(b) (3) - P.L. 86-36



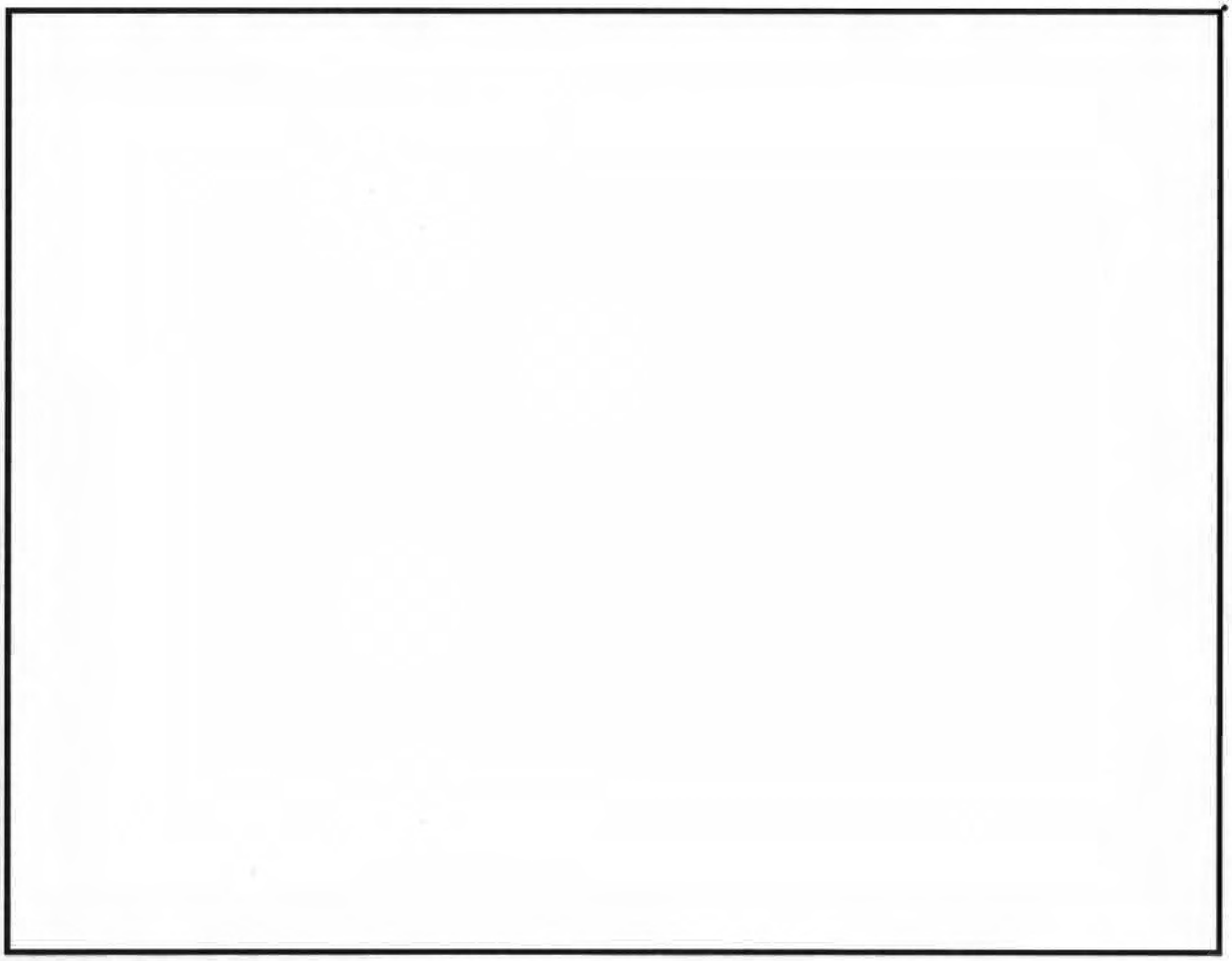
(b) (3) -P.L. 86-36

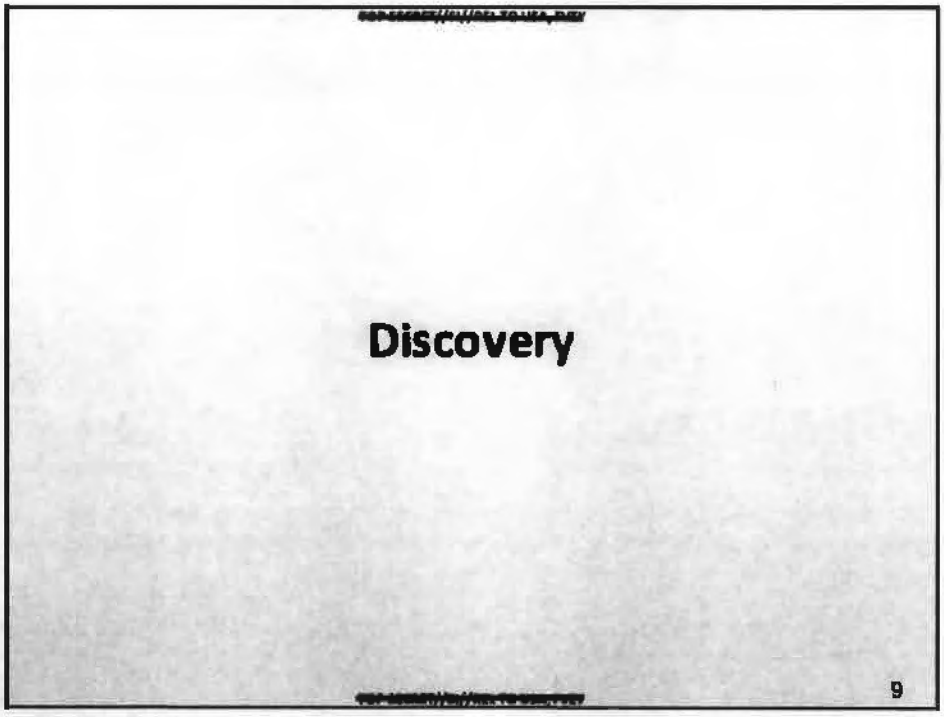




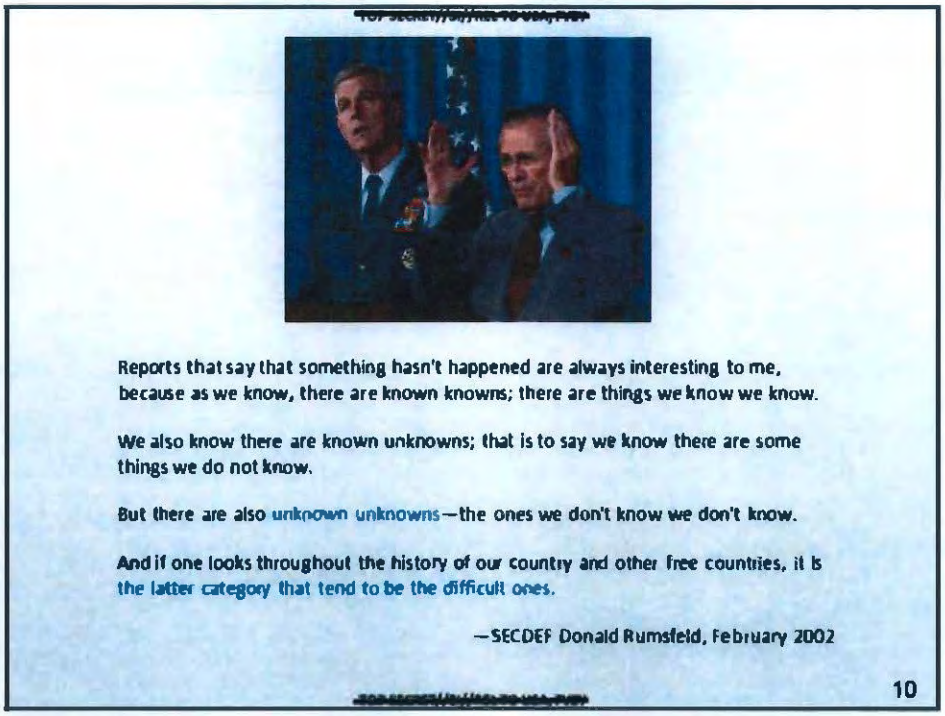
All the data processed by NSA must answer the same fundamental question: What should we keep and what should we throw away?

(b) (3)-P.L. 86-36

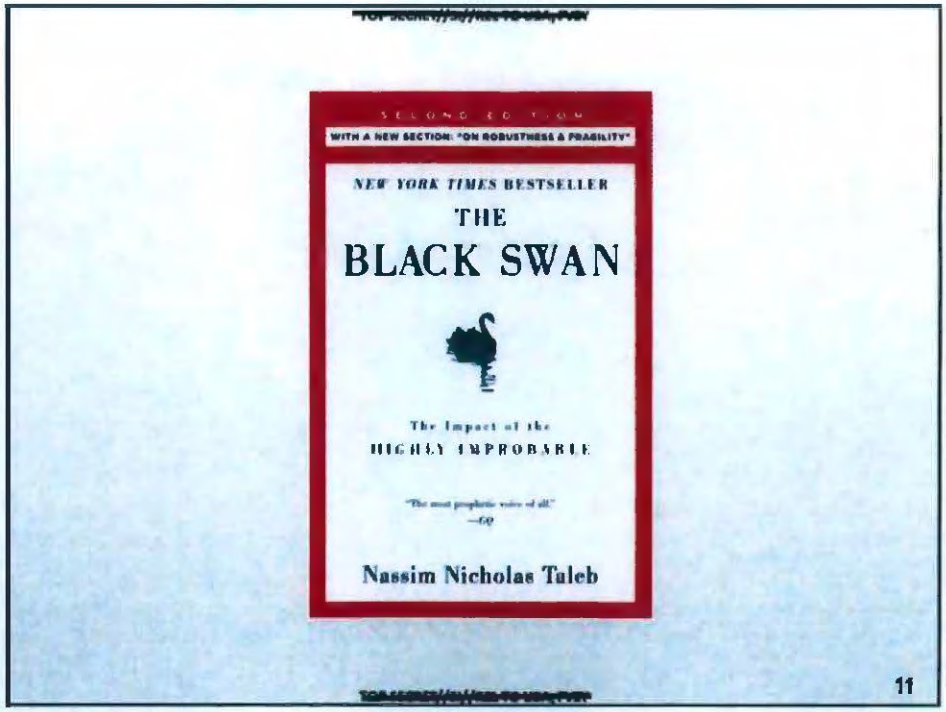




I would like to point out that we have entered the realm of discovery, a corner of the SIGINT system that hasn't always gotten the attention it deserves, but is vitally important. As we will see, the procedures and safeguards for SIGINT discovery are different from the ones for sustained mission.



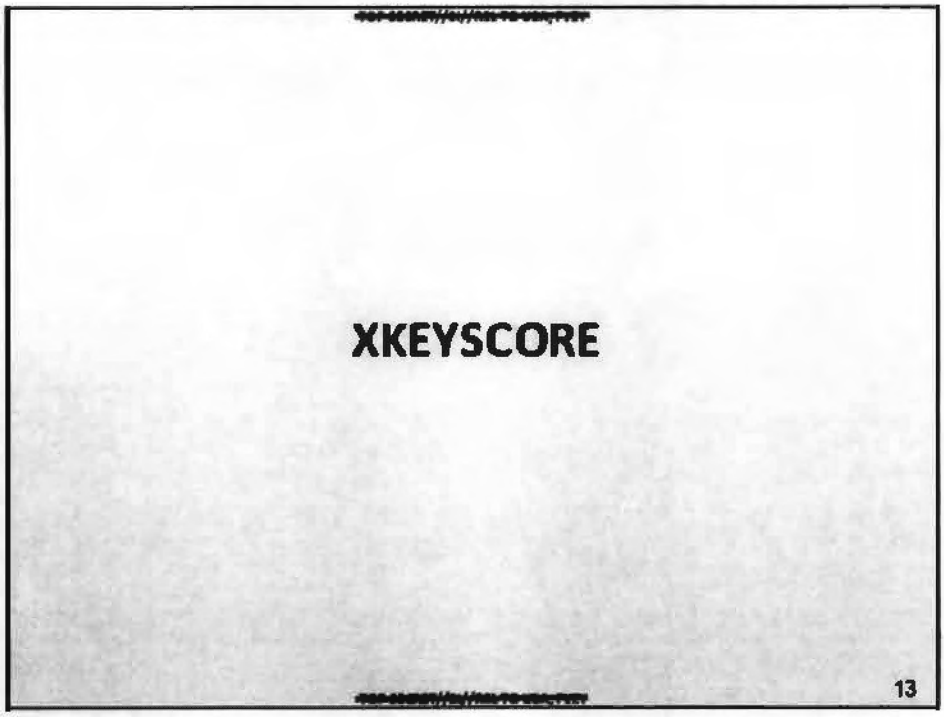
What is discovery? The best explanation is probably Donald Rumsfeld's famous quote about "unknown unknowns." In terms of SIGINT, discovery means finding new targets. If all you do is concentrate on the targets you already know about, you will soon be out of targets.



There is a related school of statistical thought that tries to prepare for "black swan" events, which are difficult to predict but possible to prepare for.

(b)(3)-P.L. 86-36

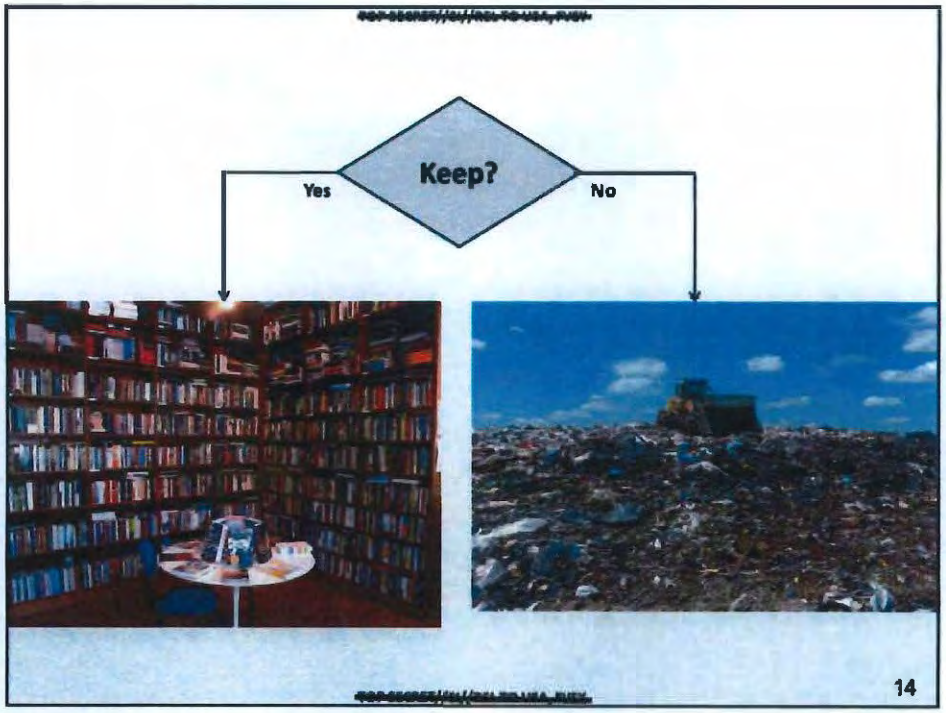
12



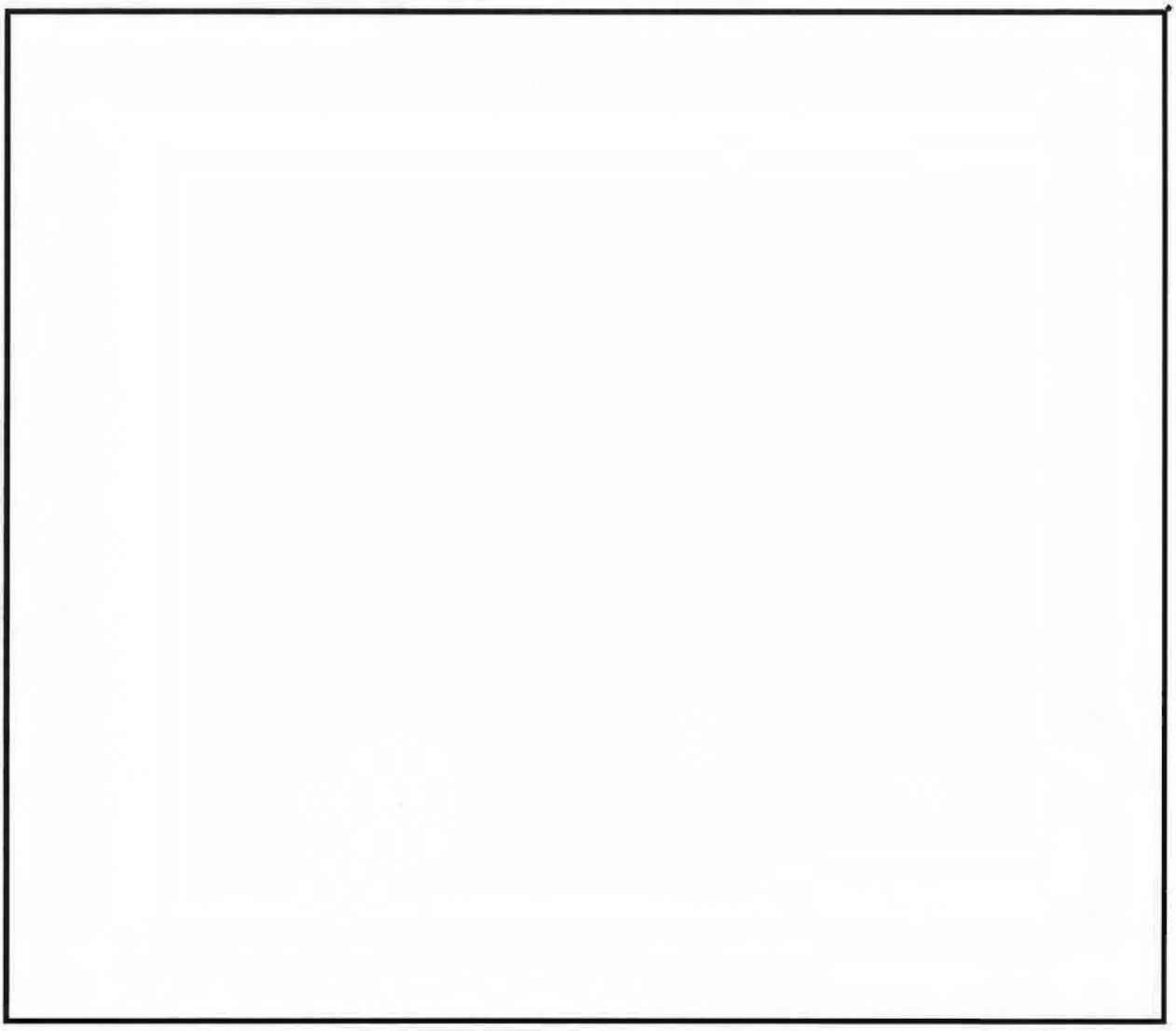
XKEYSCORE [redacted] It is NSA main tool for discovery.

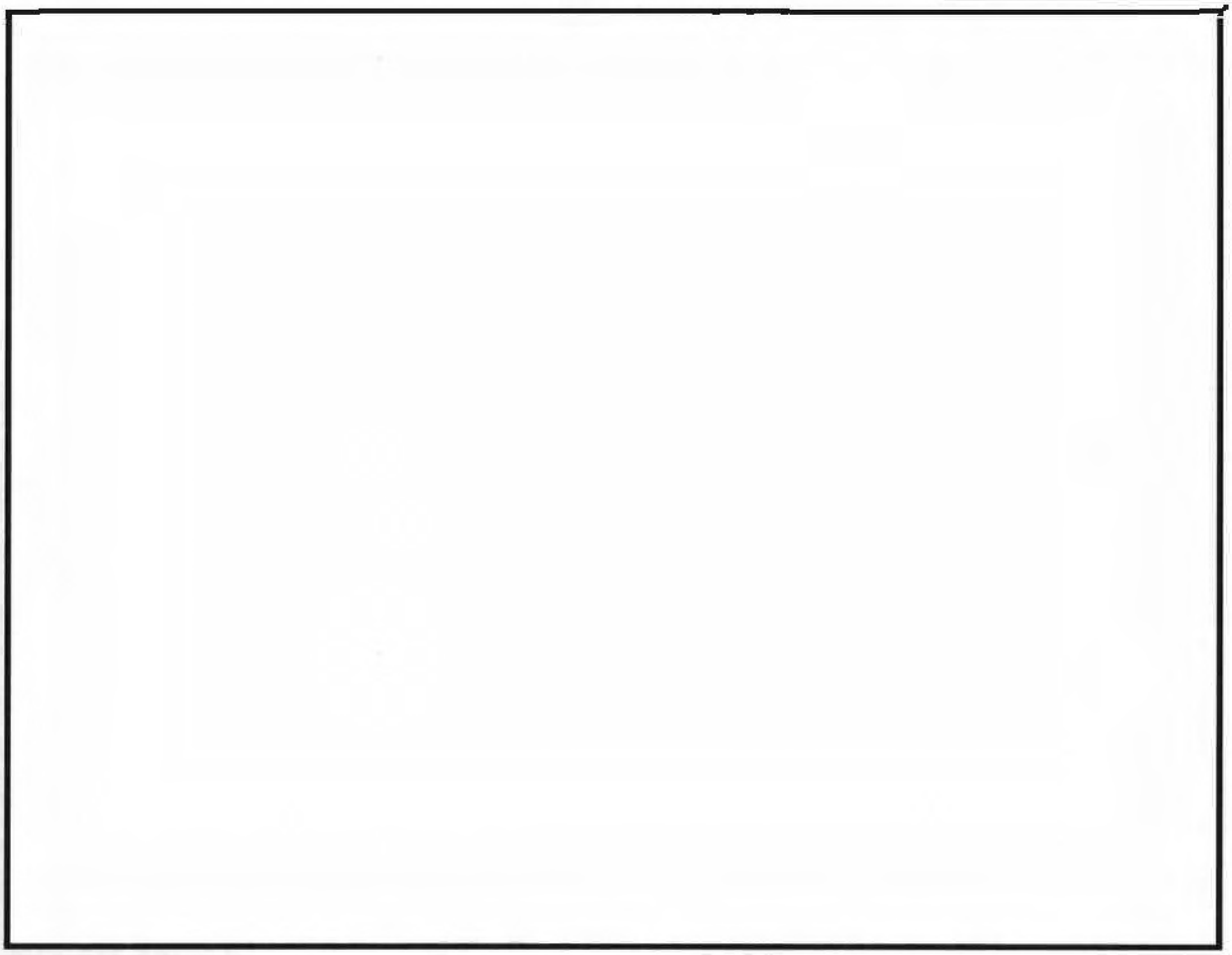
(b) (3)-P.L. 86-36

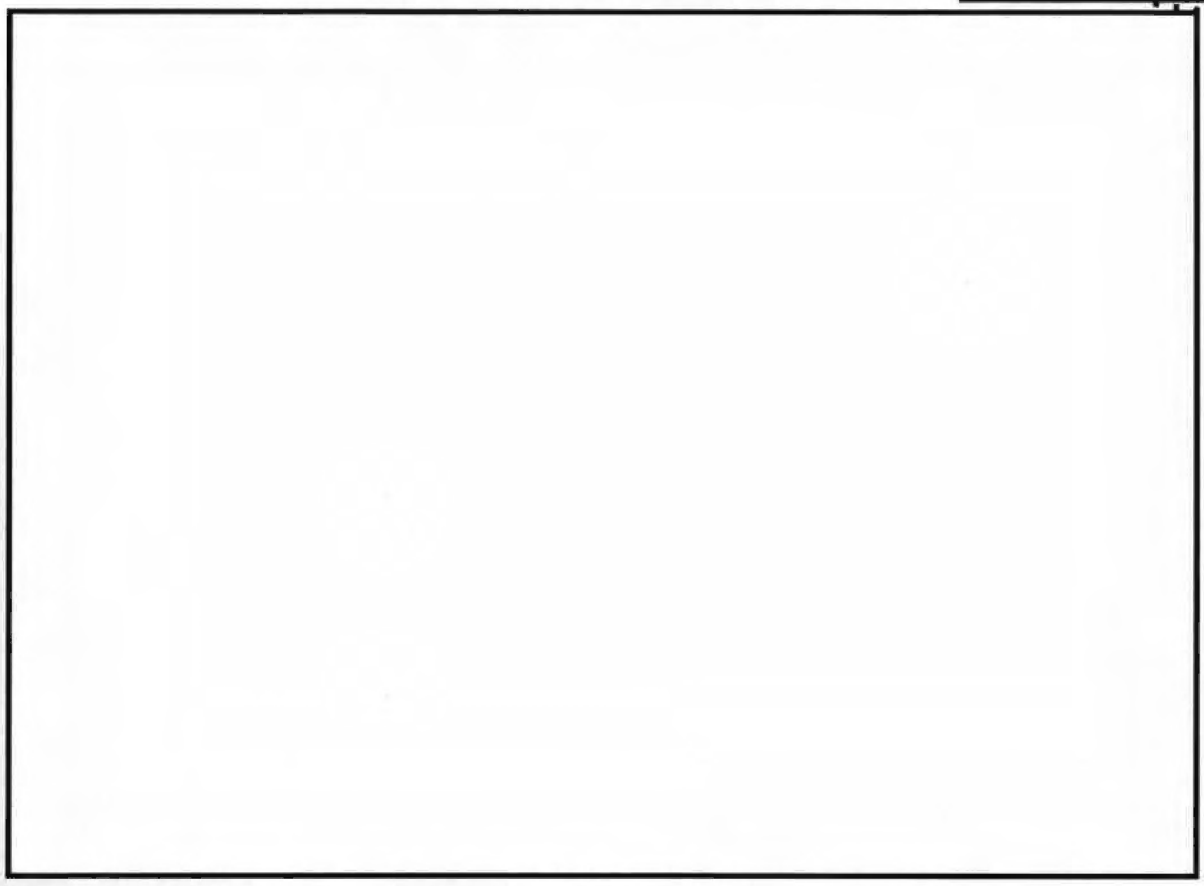
(b) (3)-P.L. 86-36

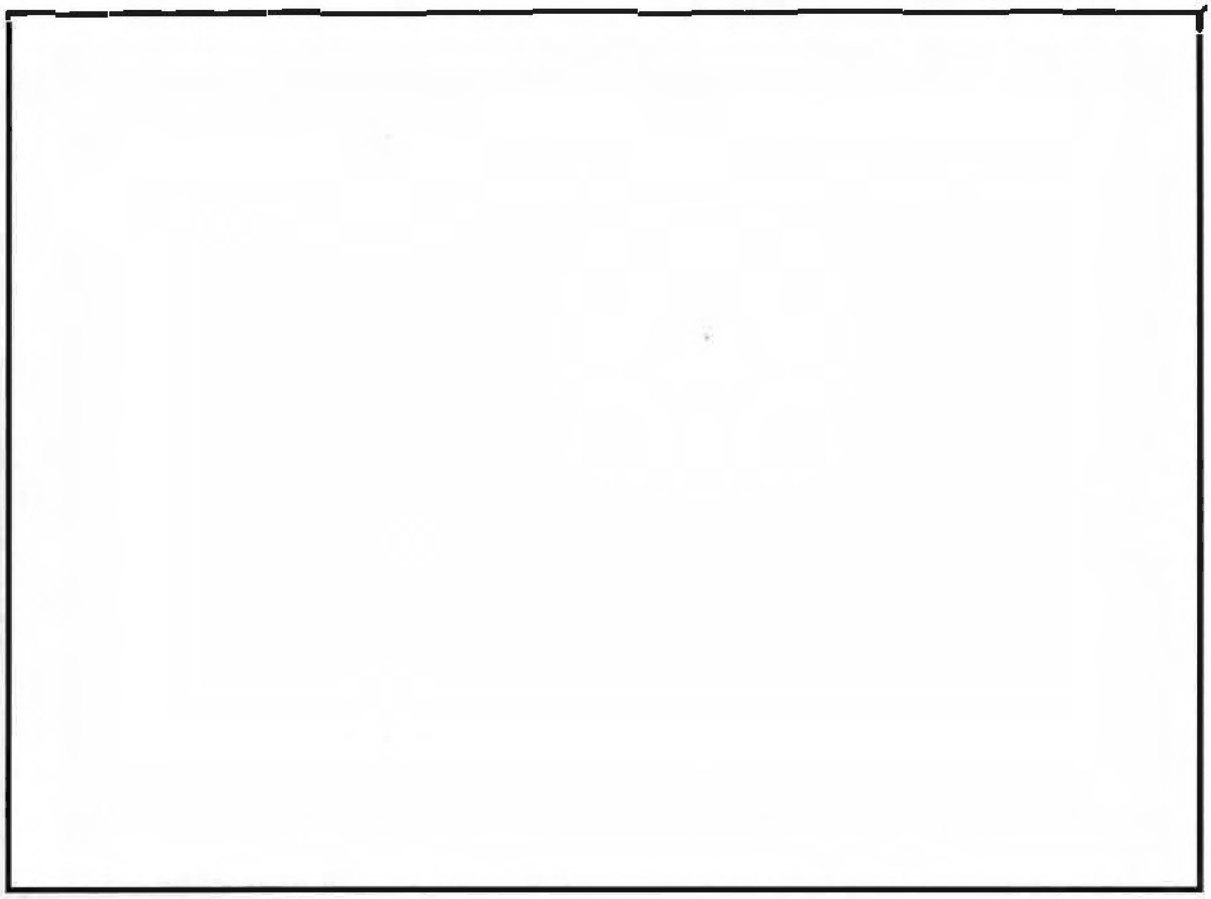


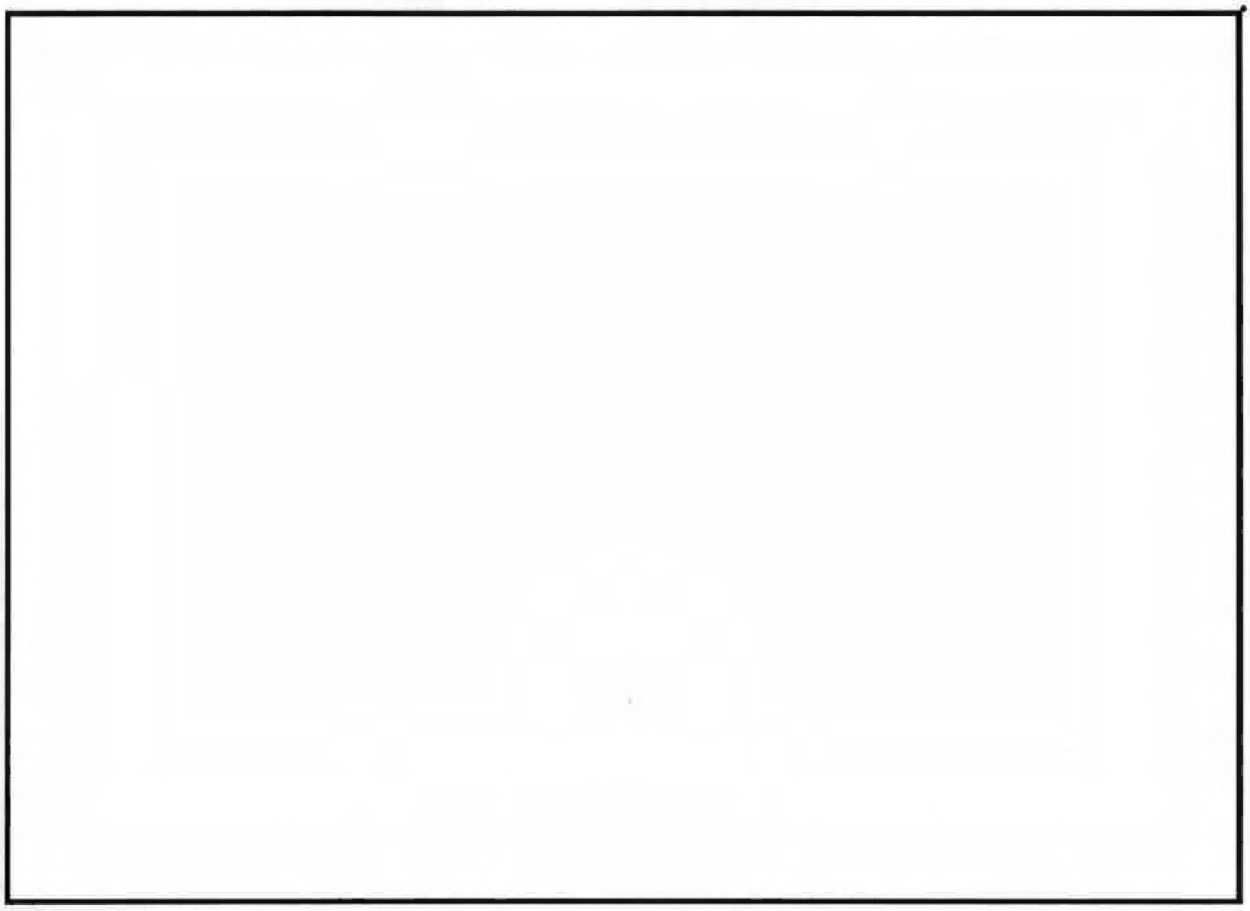
(b) (3) -P.L. 86-36

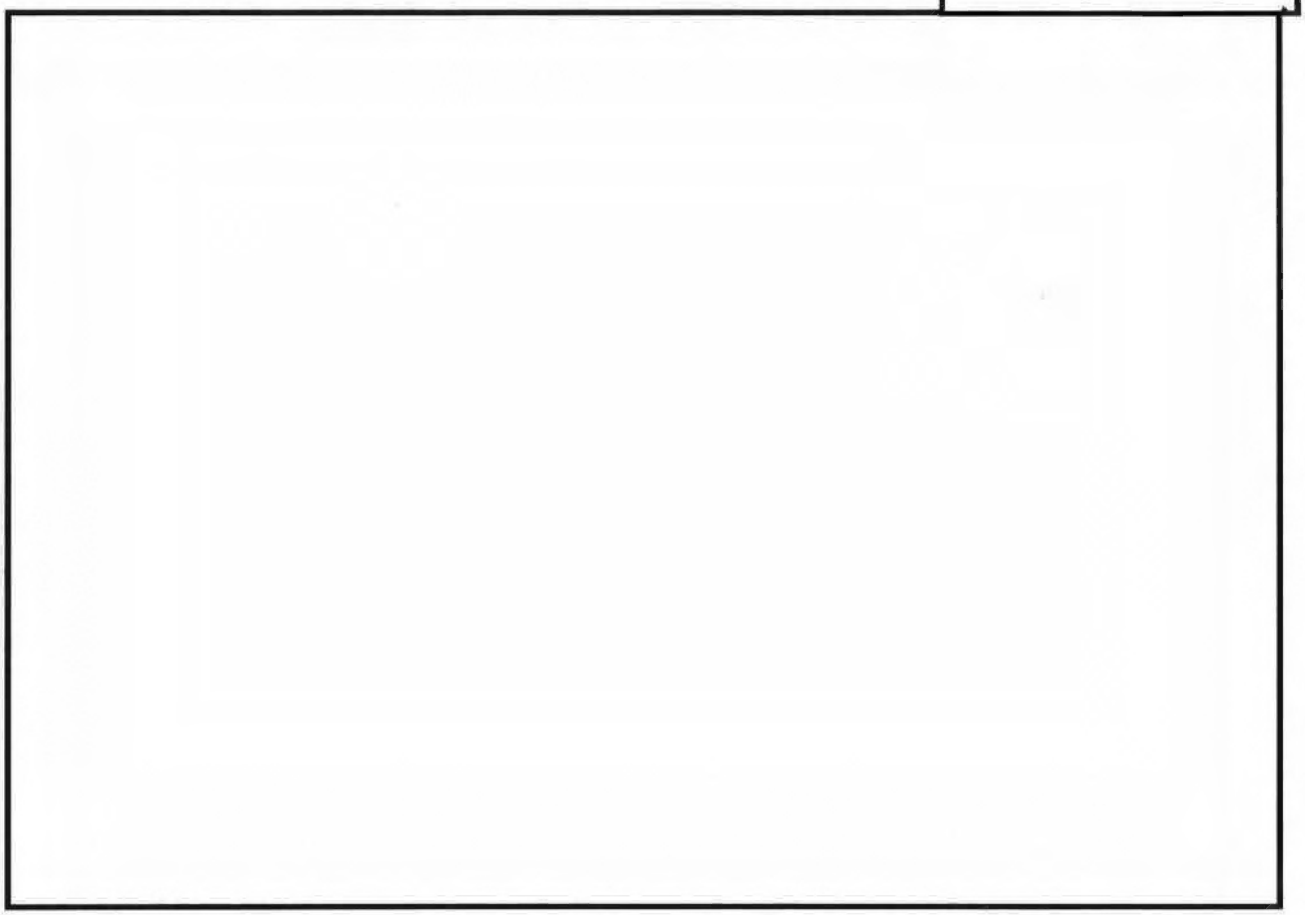


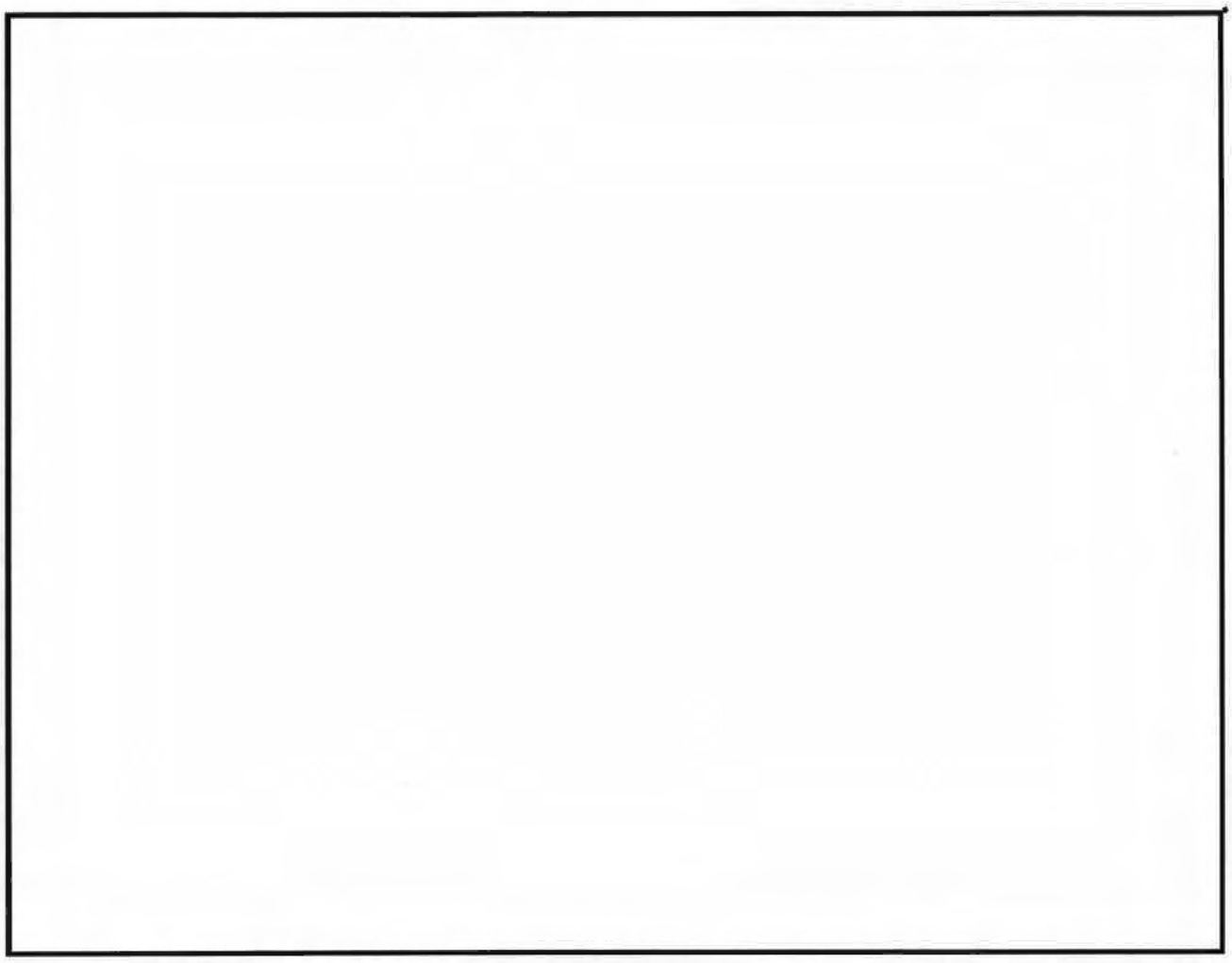


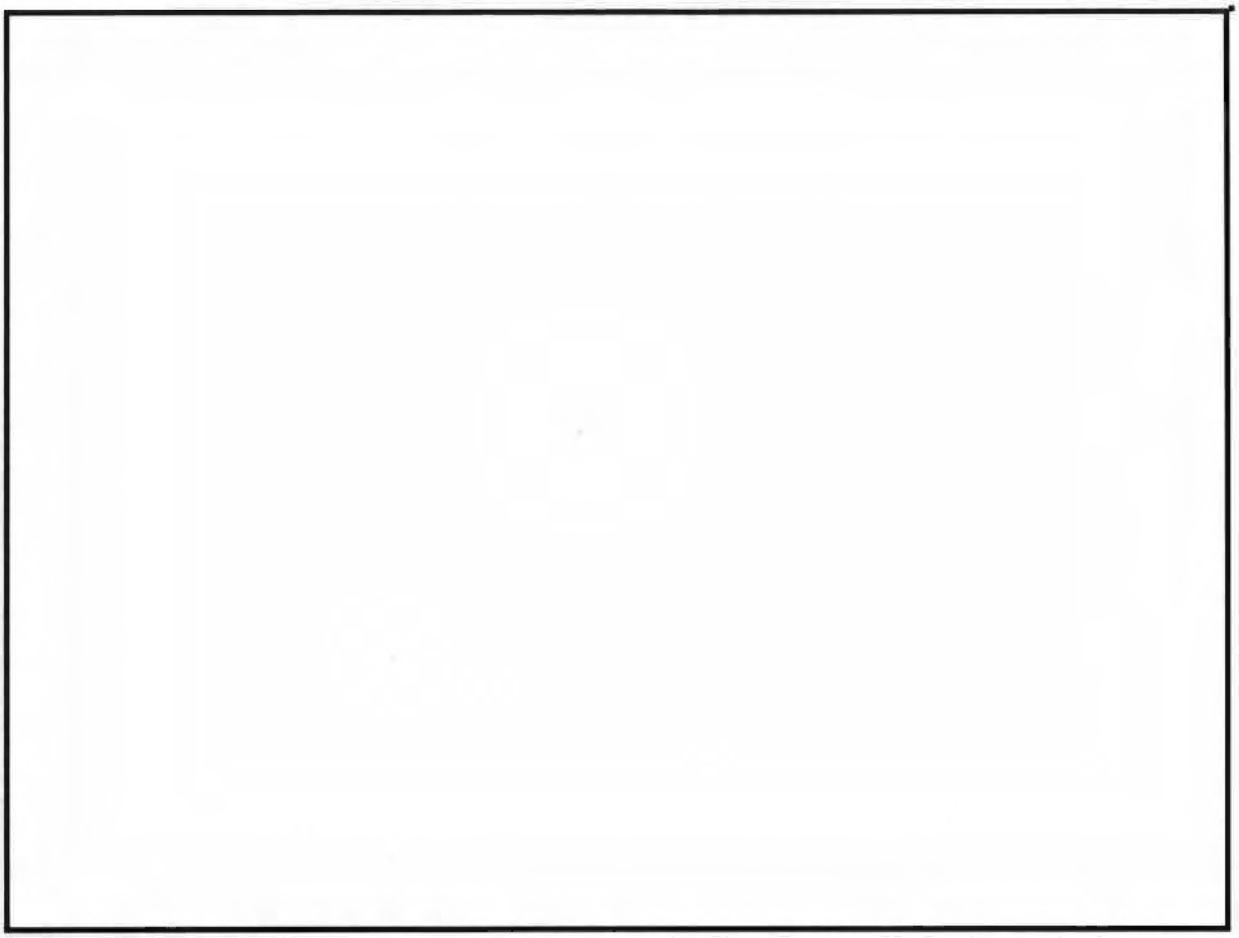


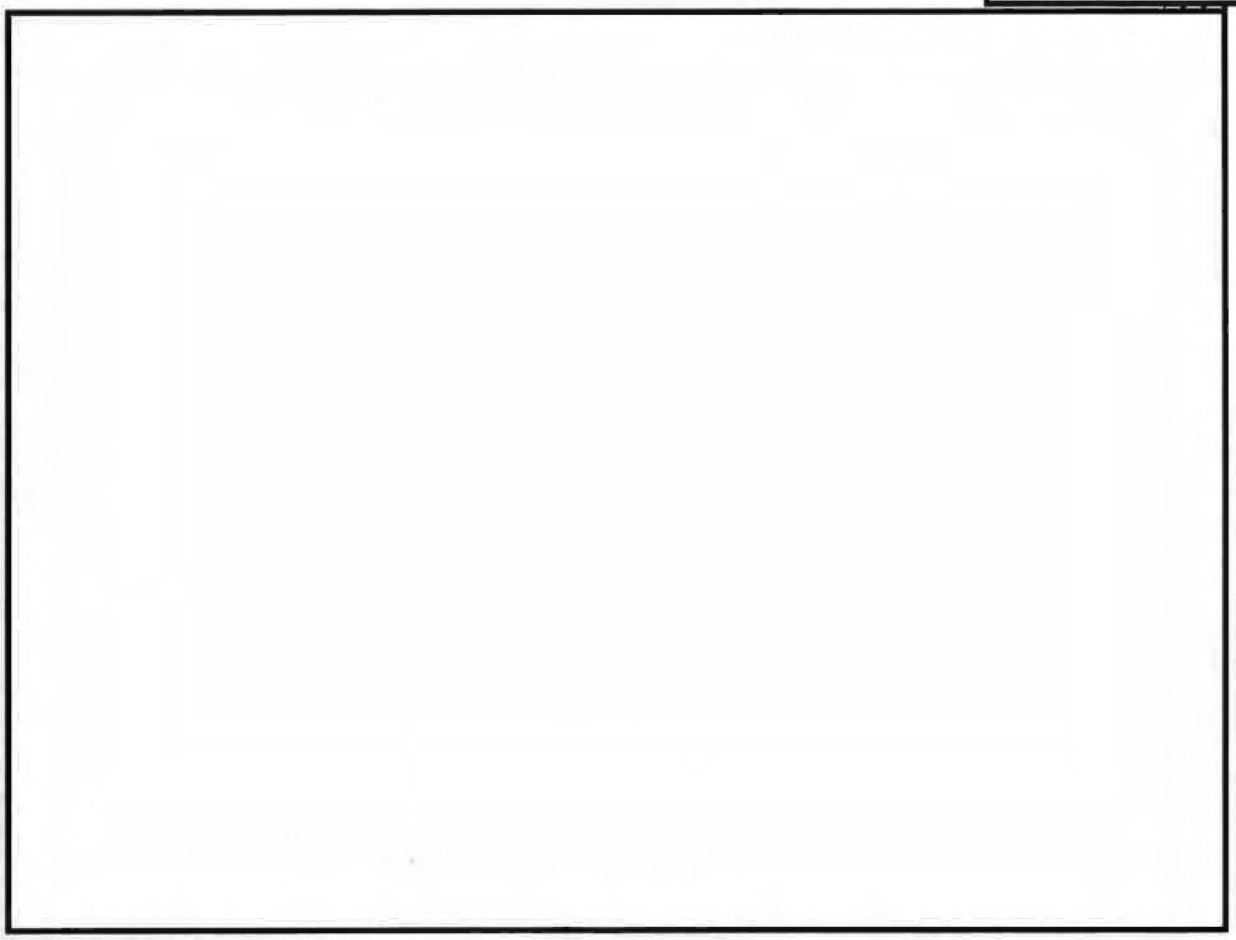


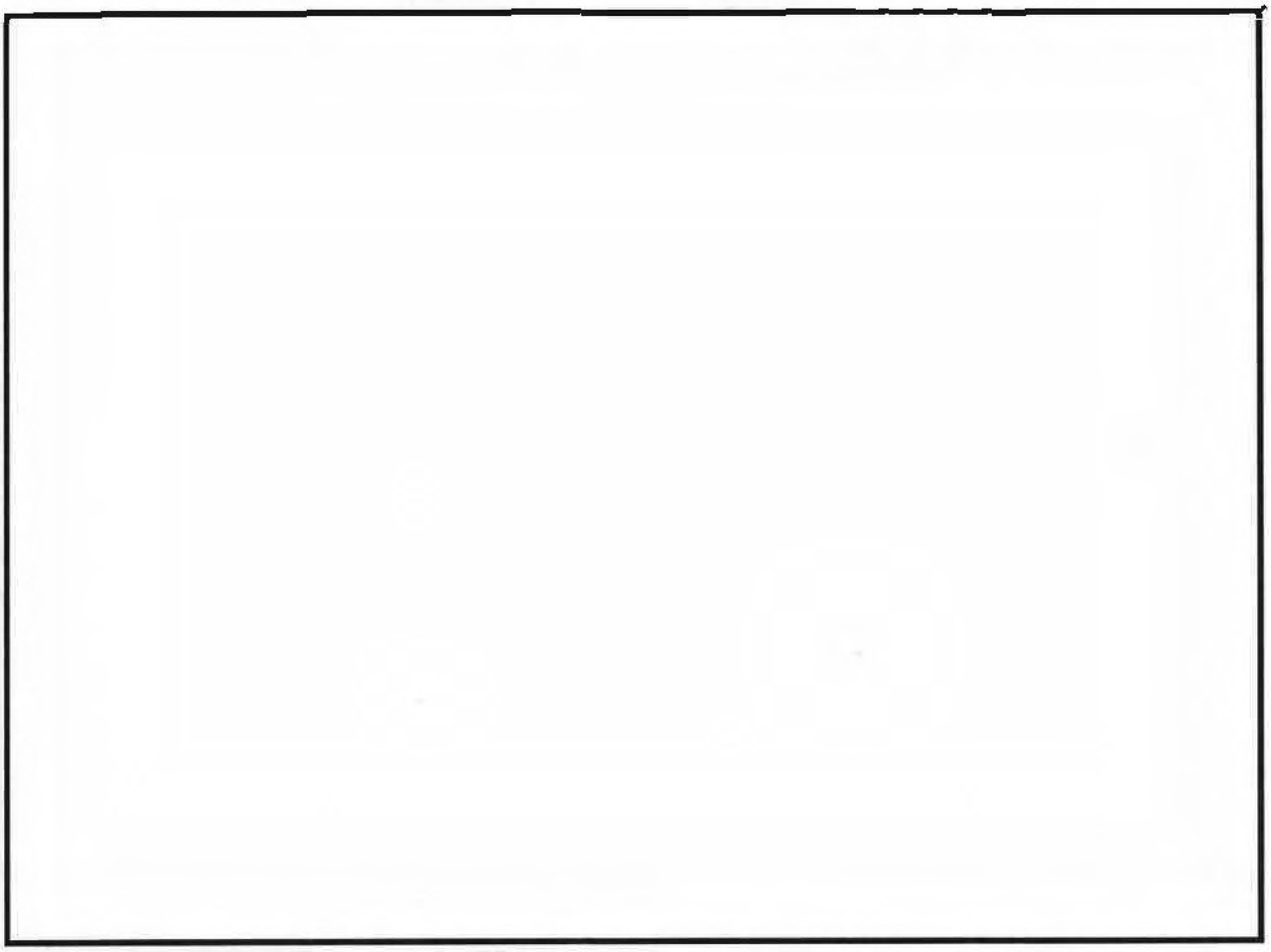


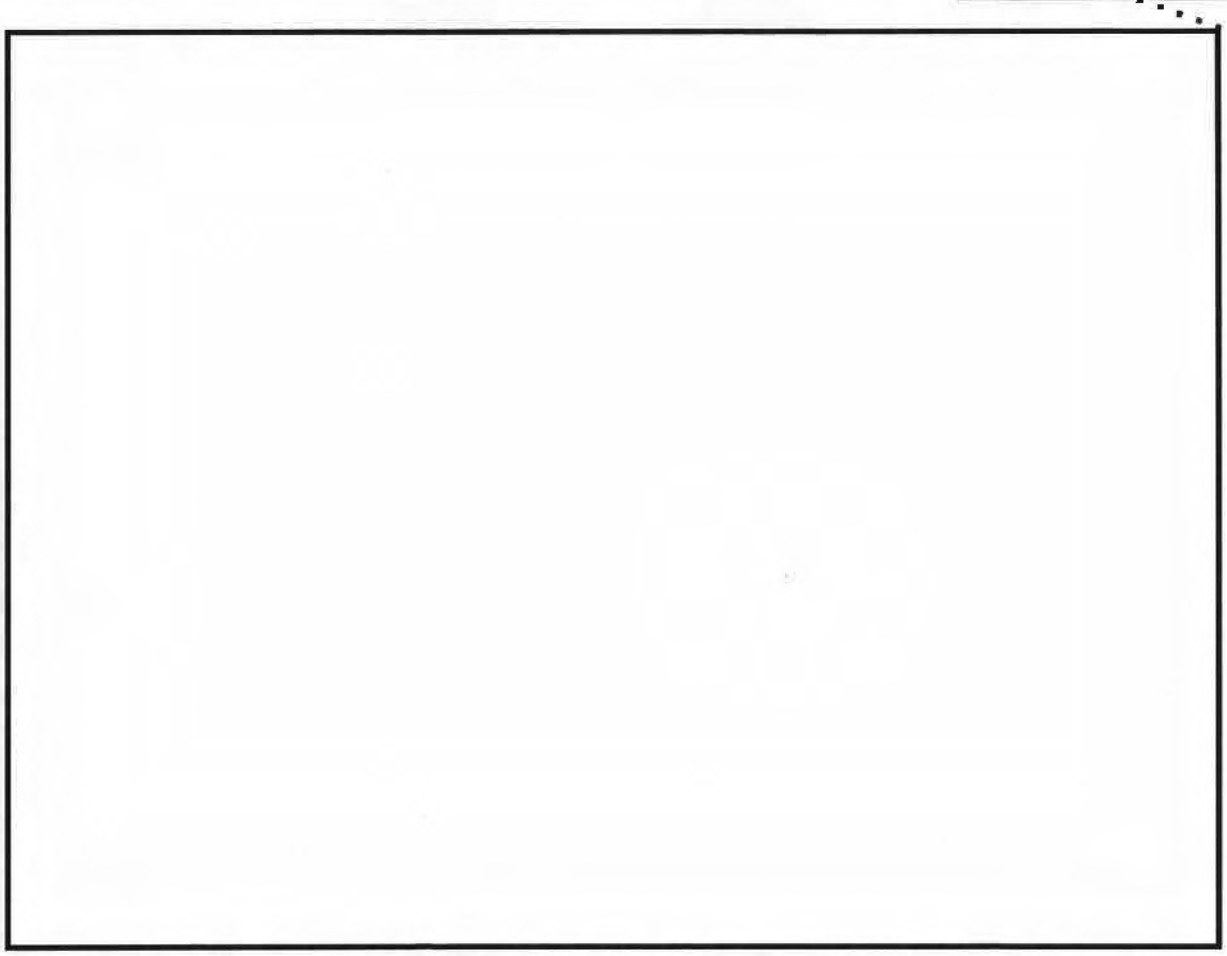


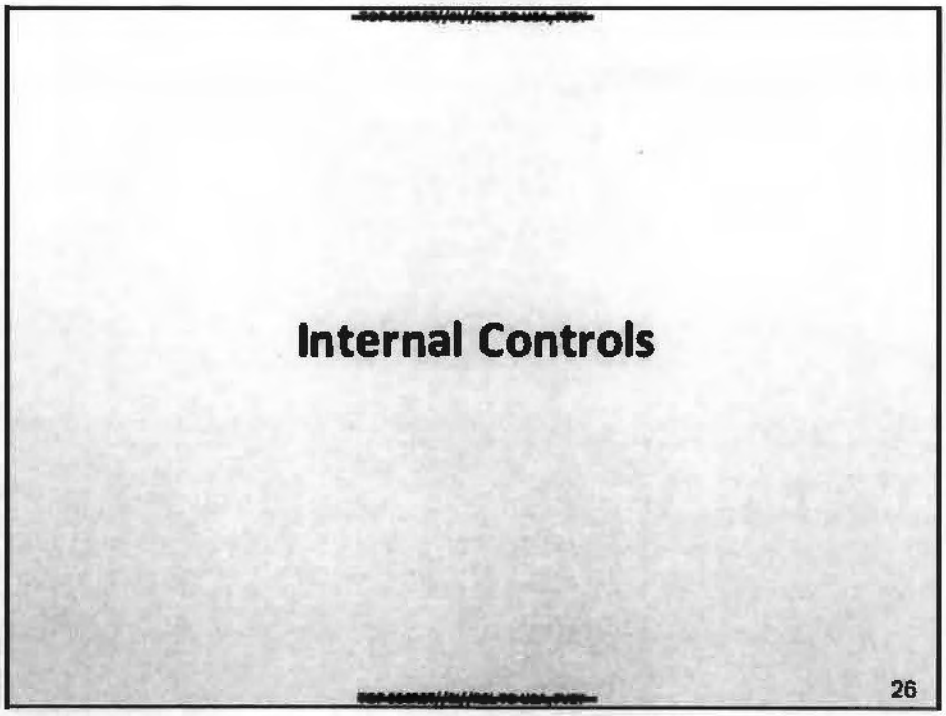






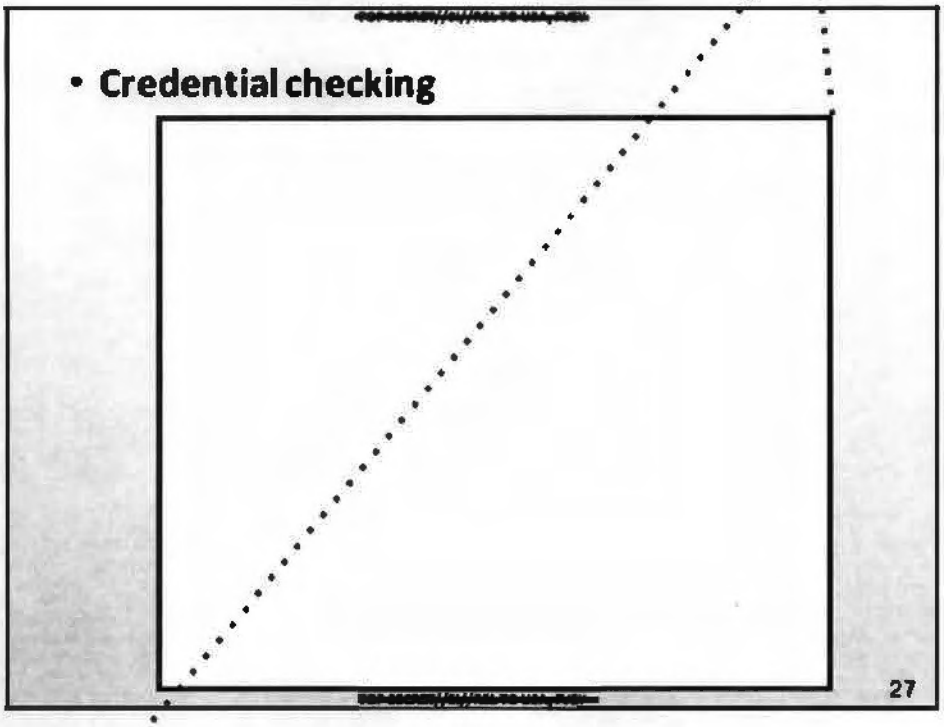




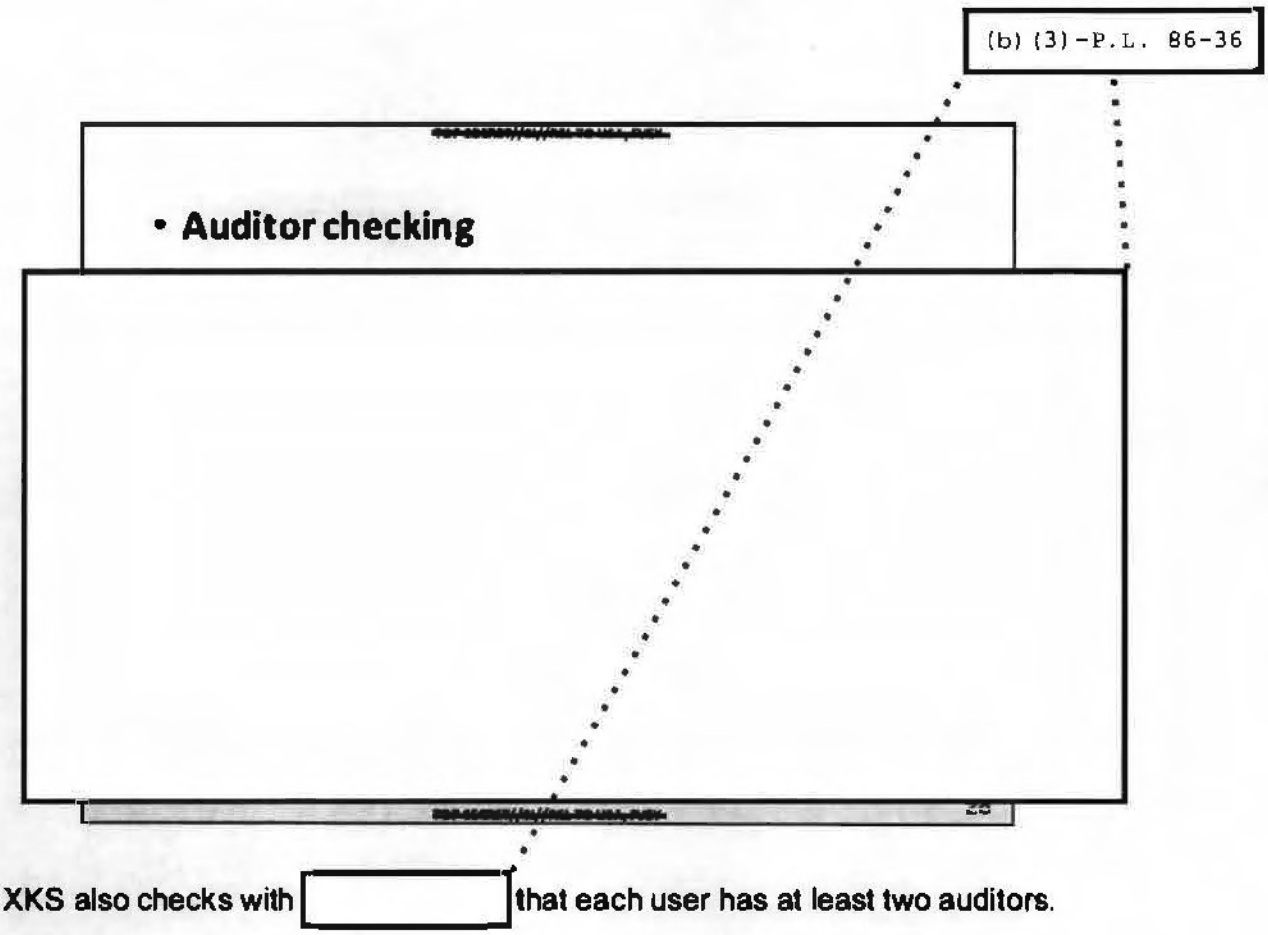


XKEYSCORE has a number of features designed to ensure compliance with laws, regulations, and policies.

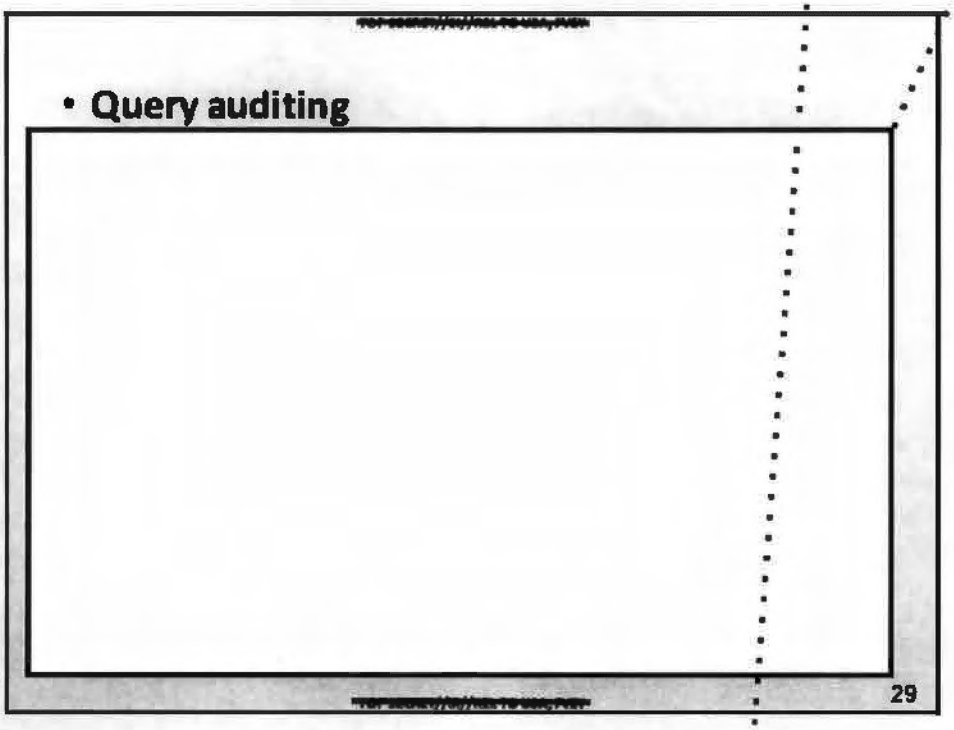
(b)(3)-P.L. 86-36



First off, before a user can even get into the tool, his credentials are checked in

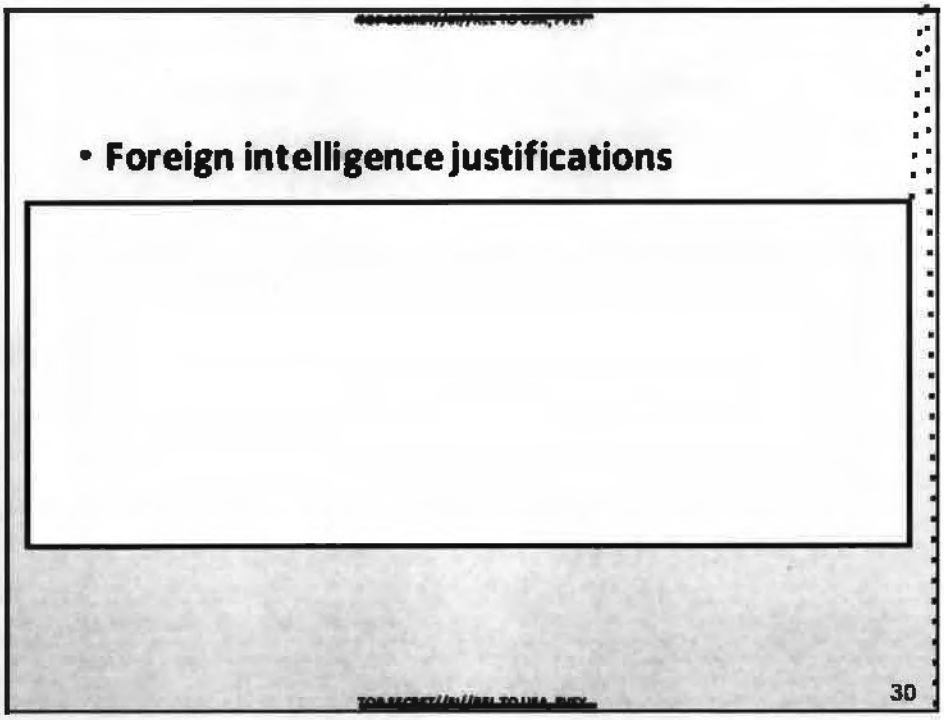

(b) (3)-P.L. 86-36
• Auditor checking
XKS also checks with
that each user has at least two auditors.

(b)(3)-P.L. 86-36



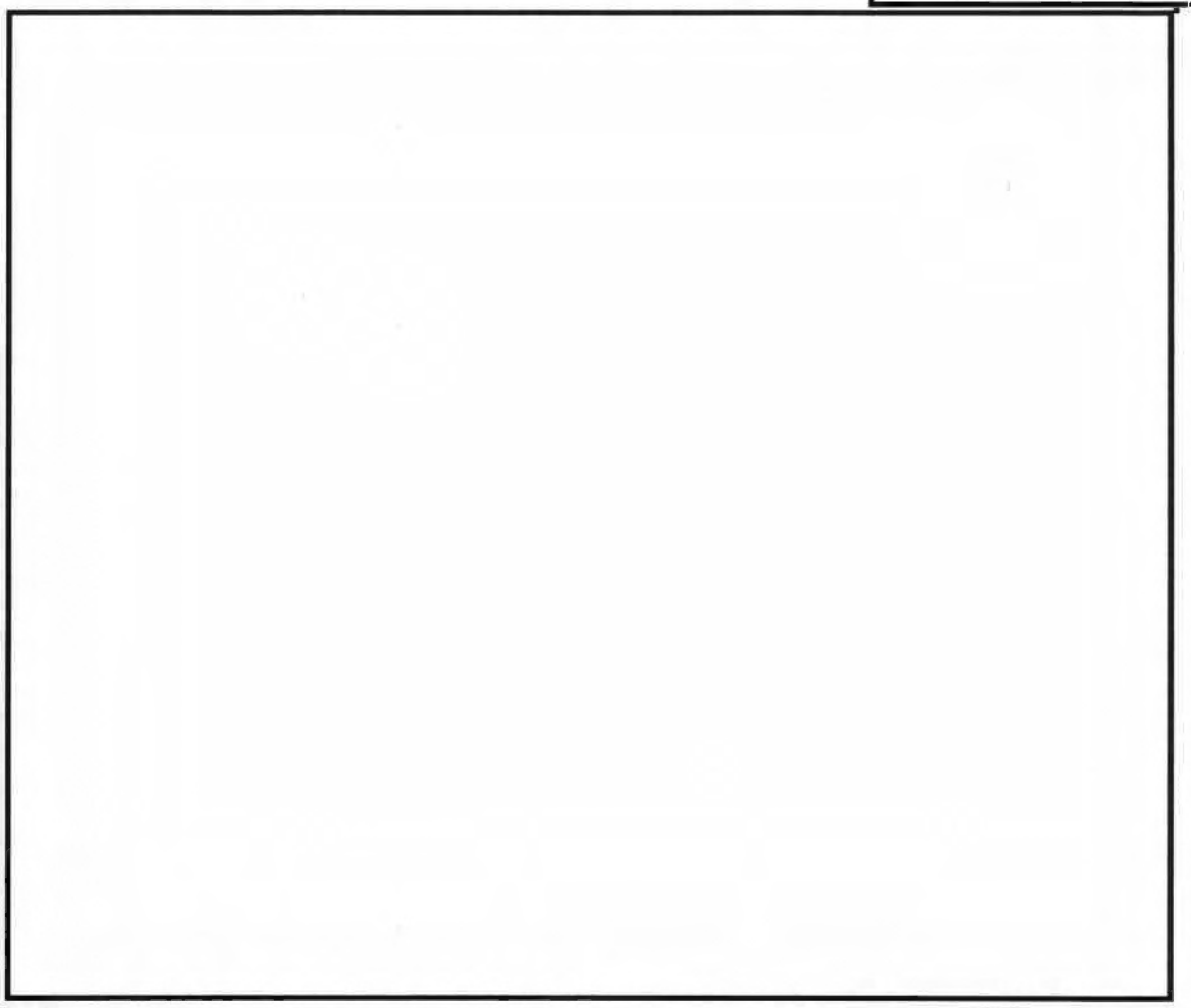
All queries are logged and made available to for audit. The auditor must review all queries made

(b)(3)-P.L. 86-36

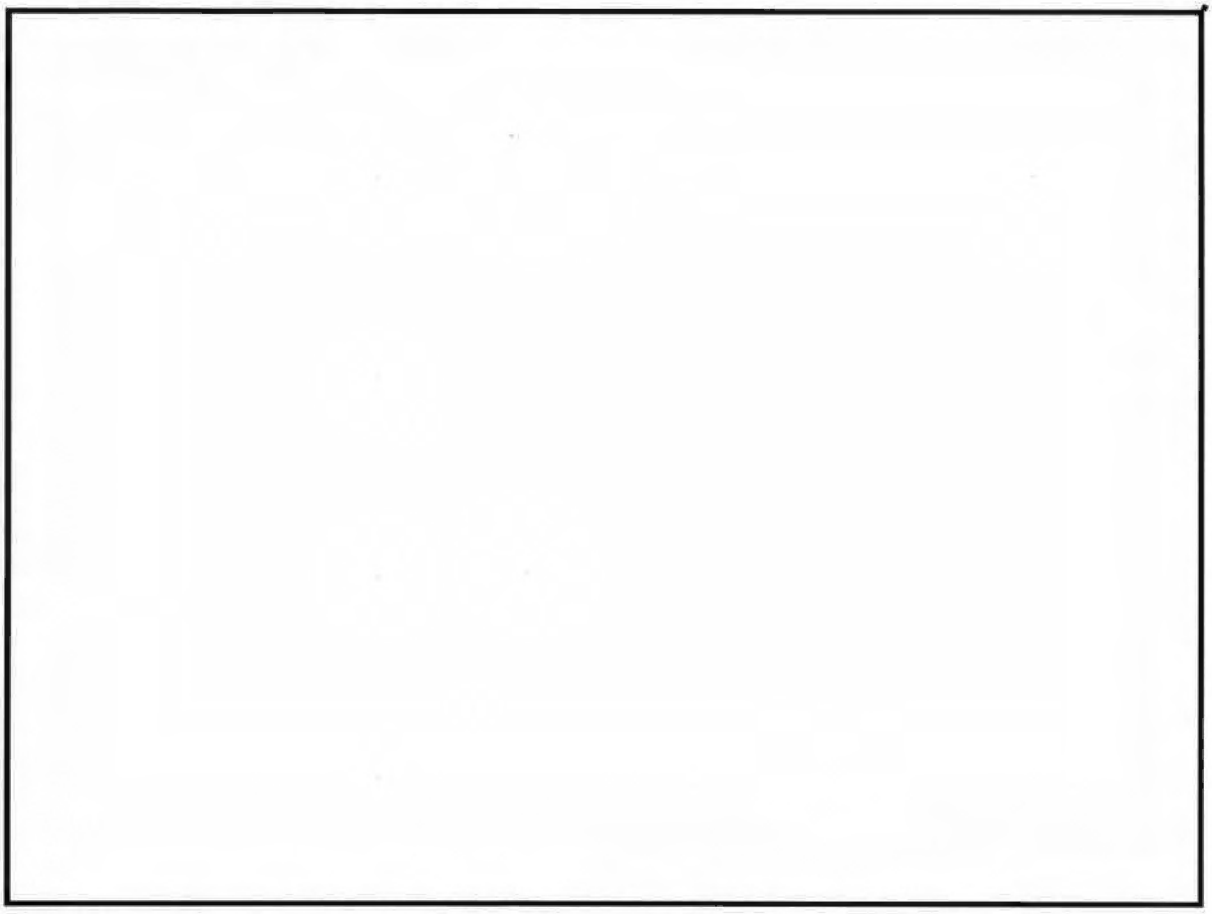


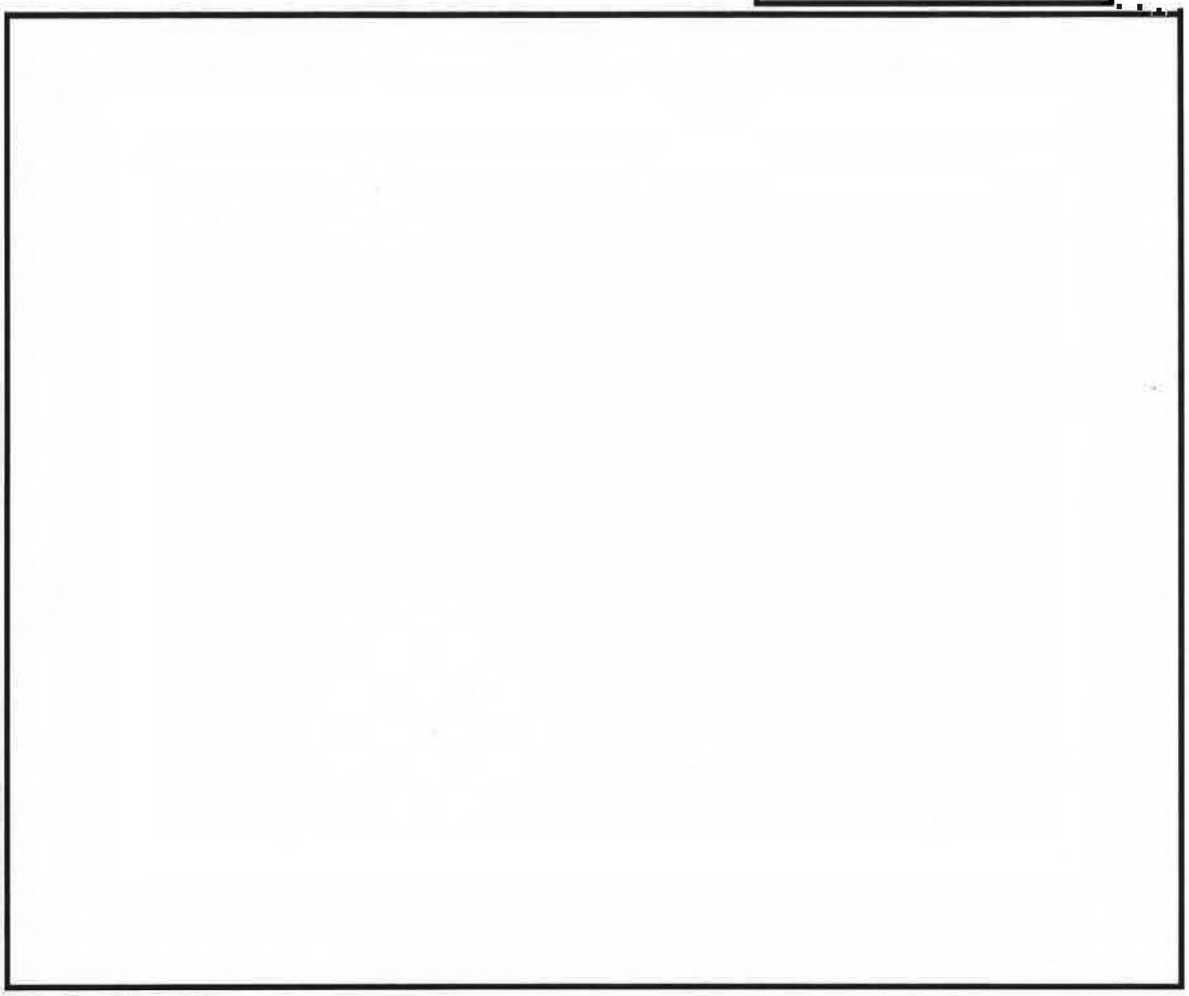
Each query must have a justification. These are included in the audit logs.

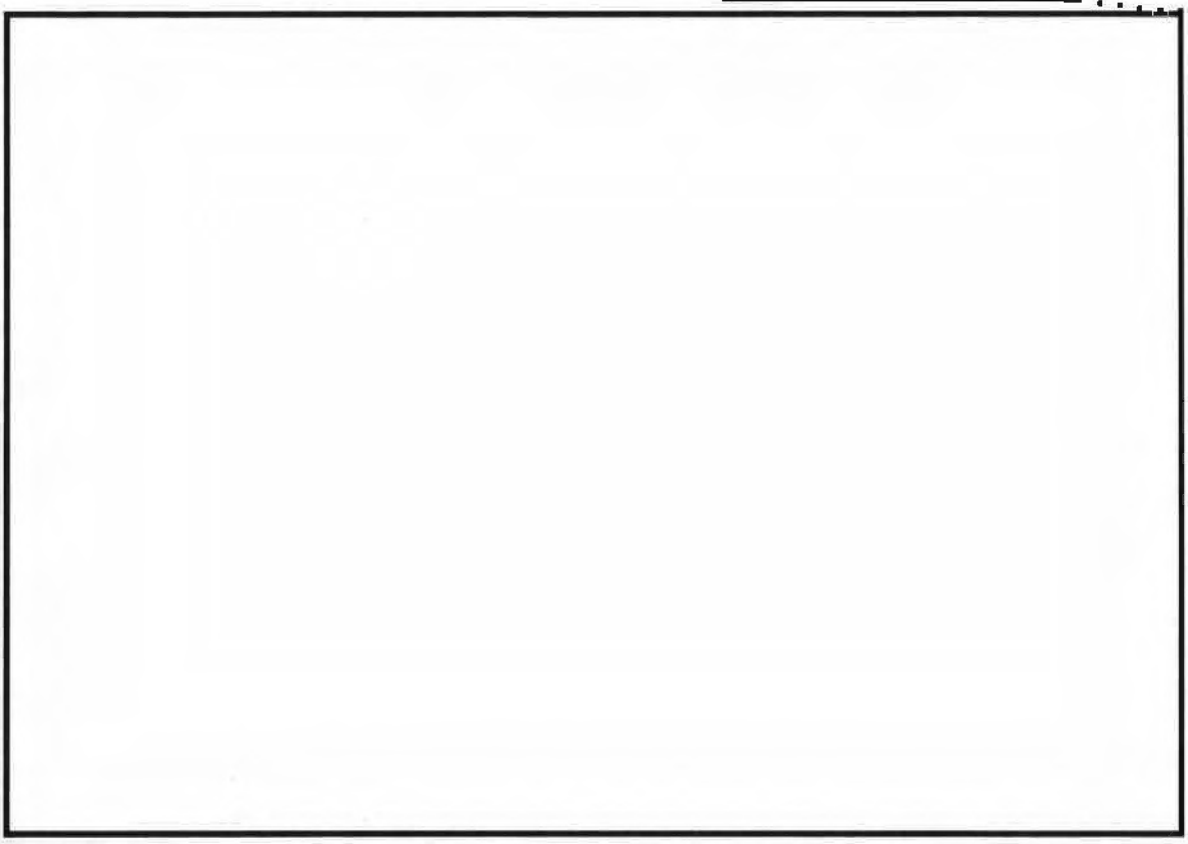
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

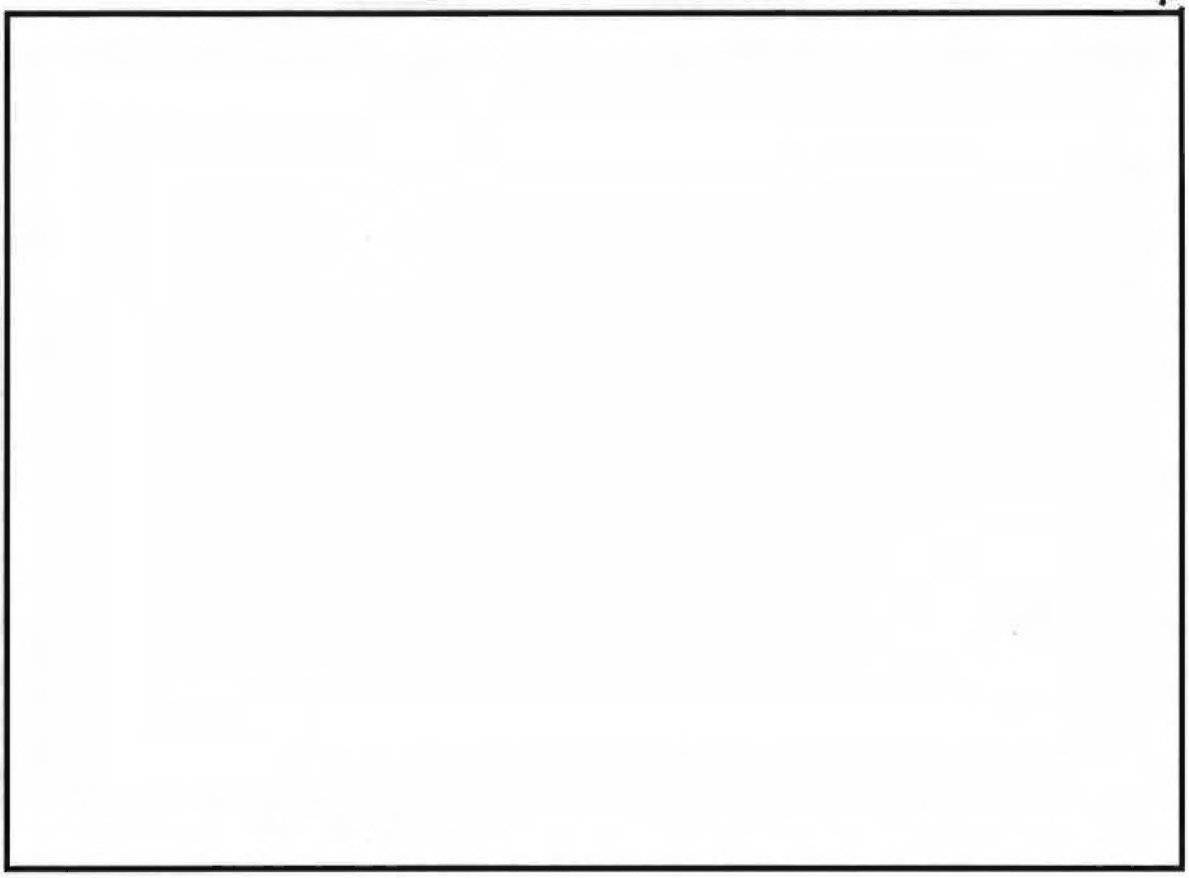


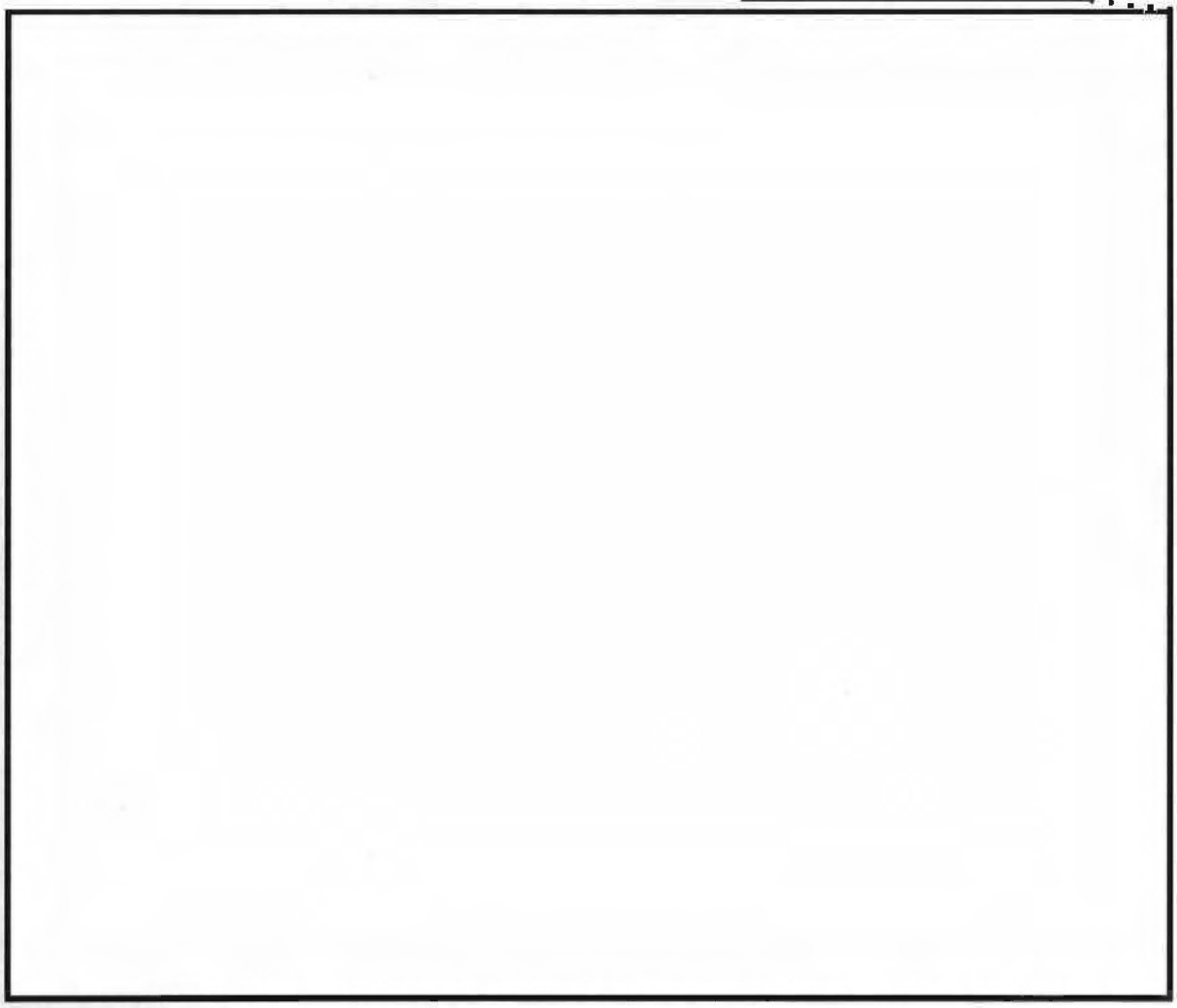
(b) (3)-P.L. 86-36



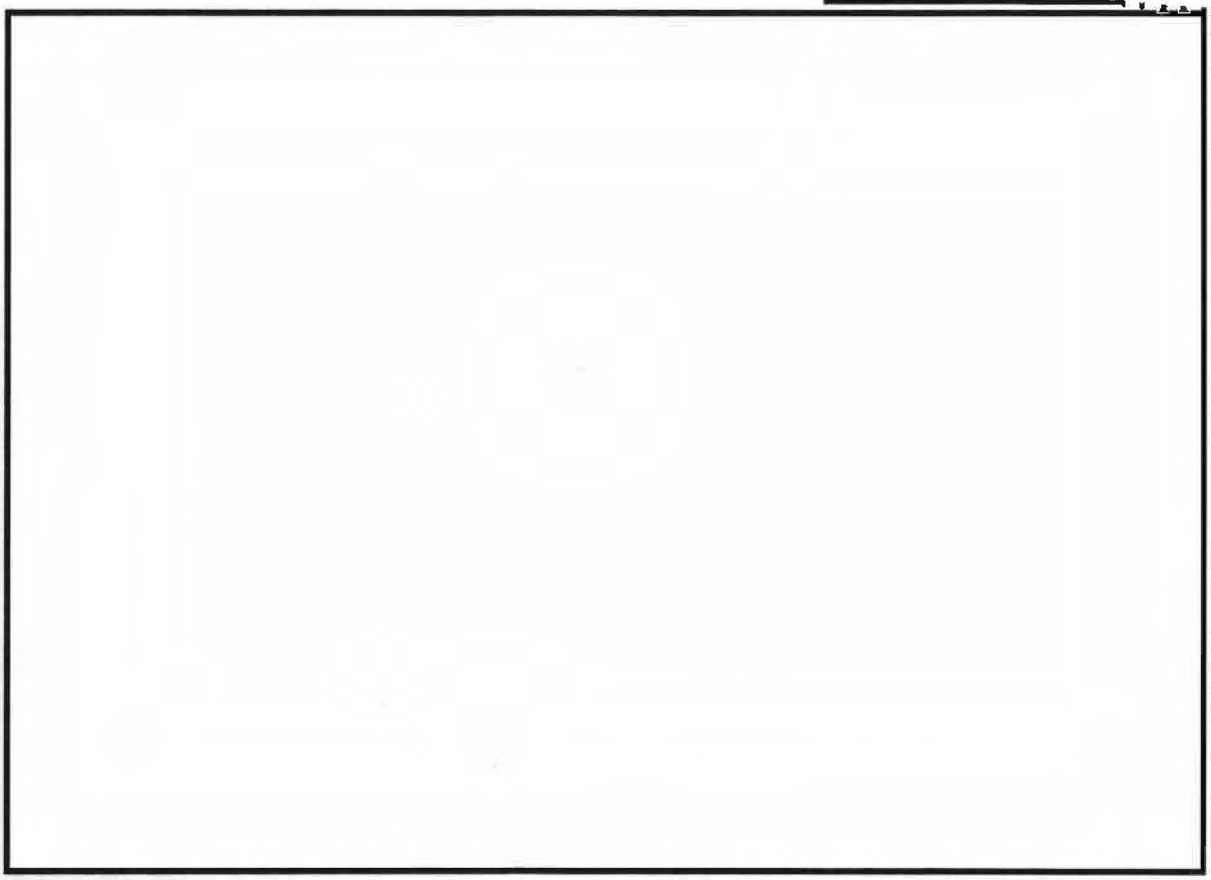




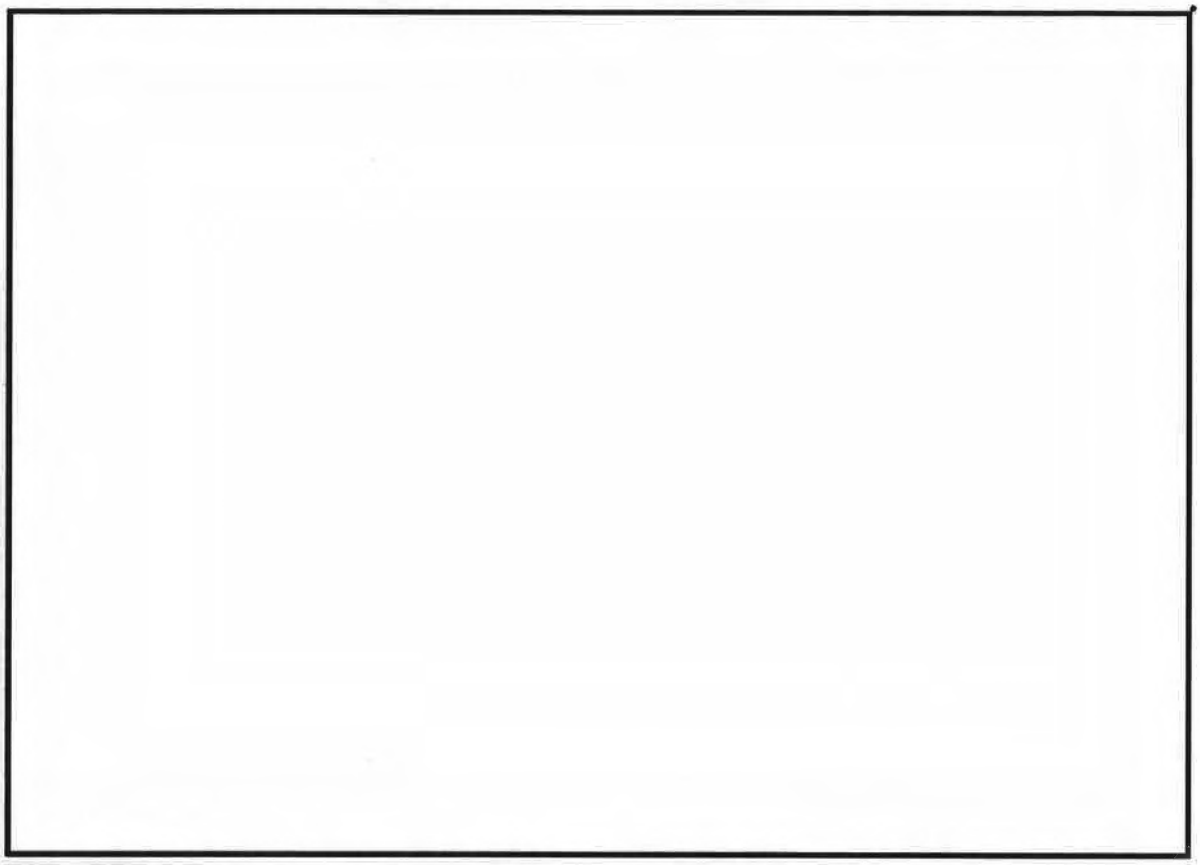


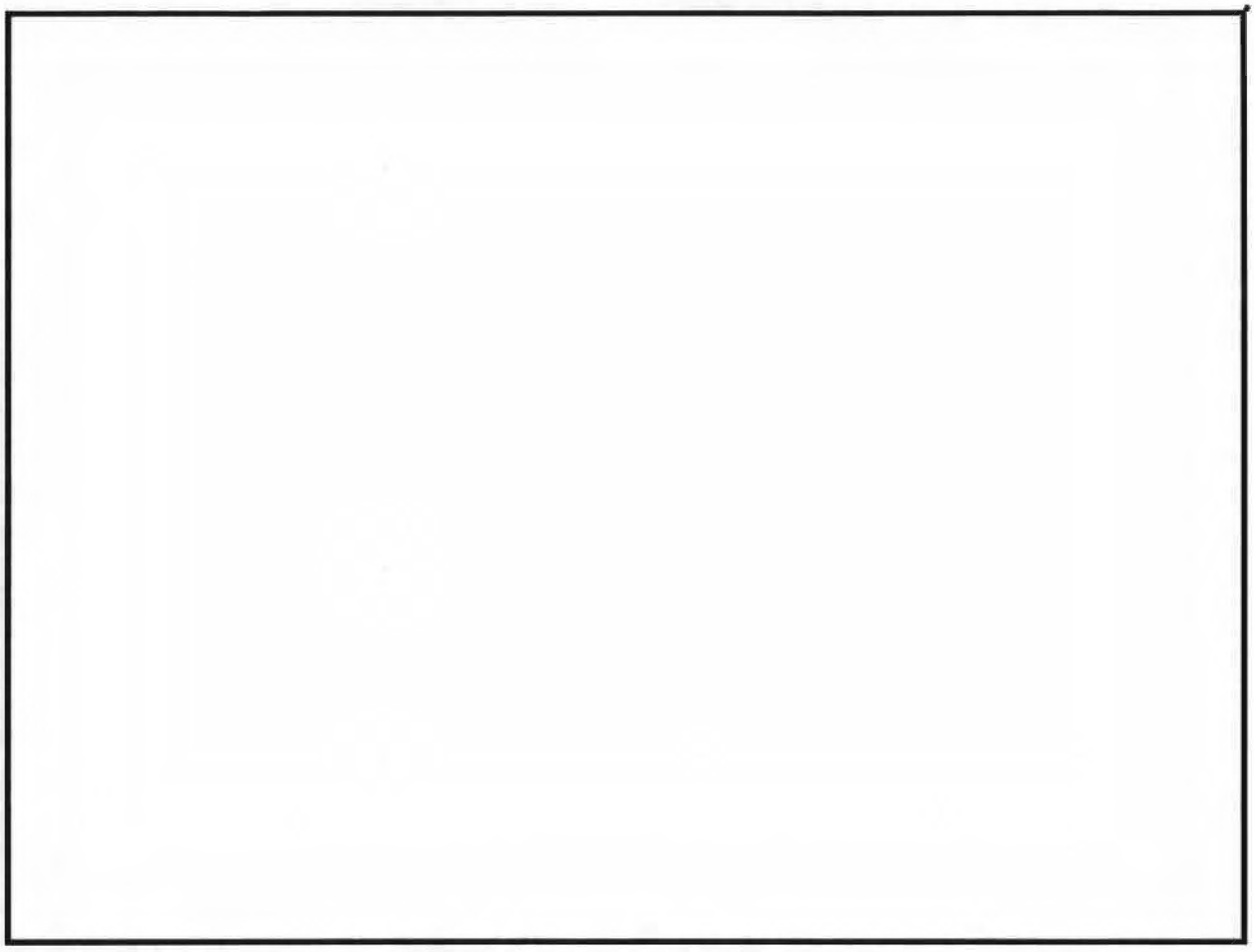


(b)(3)-P.L. 86-36

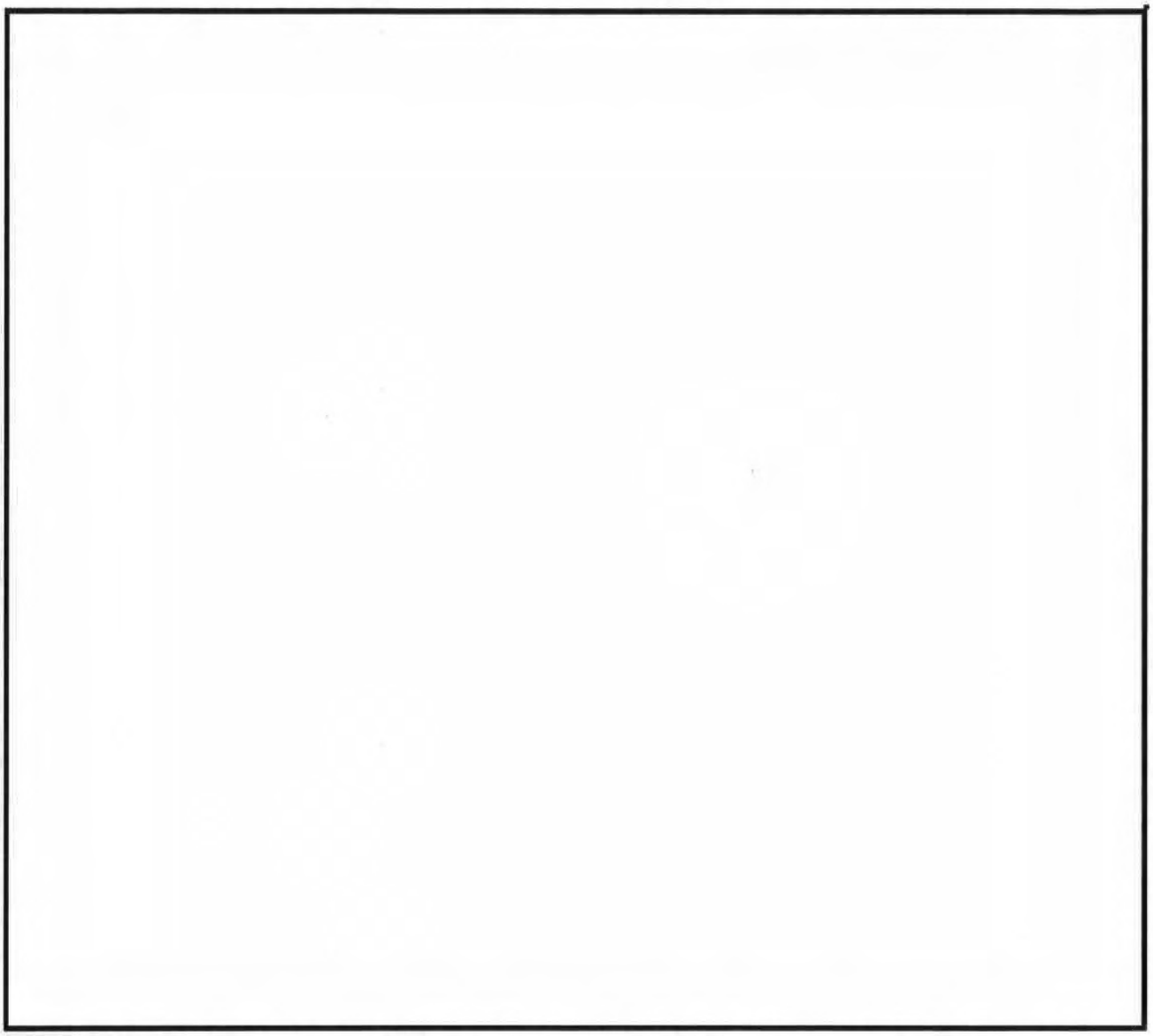


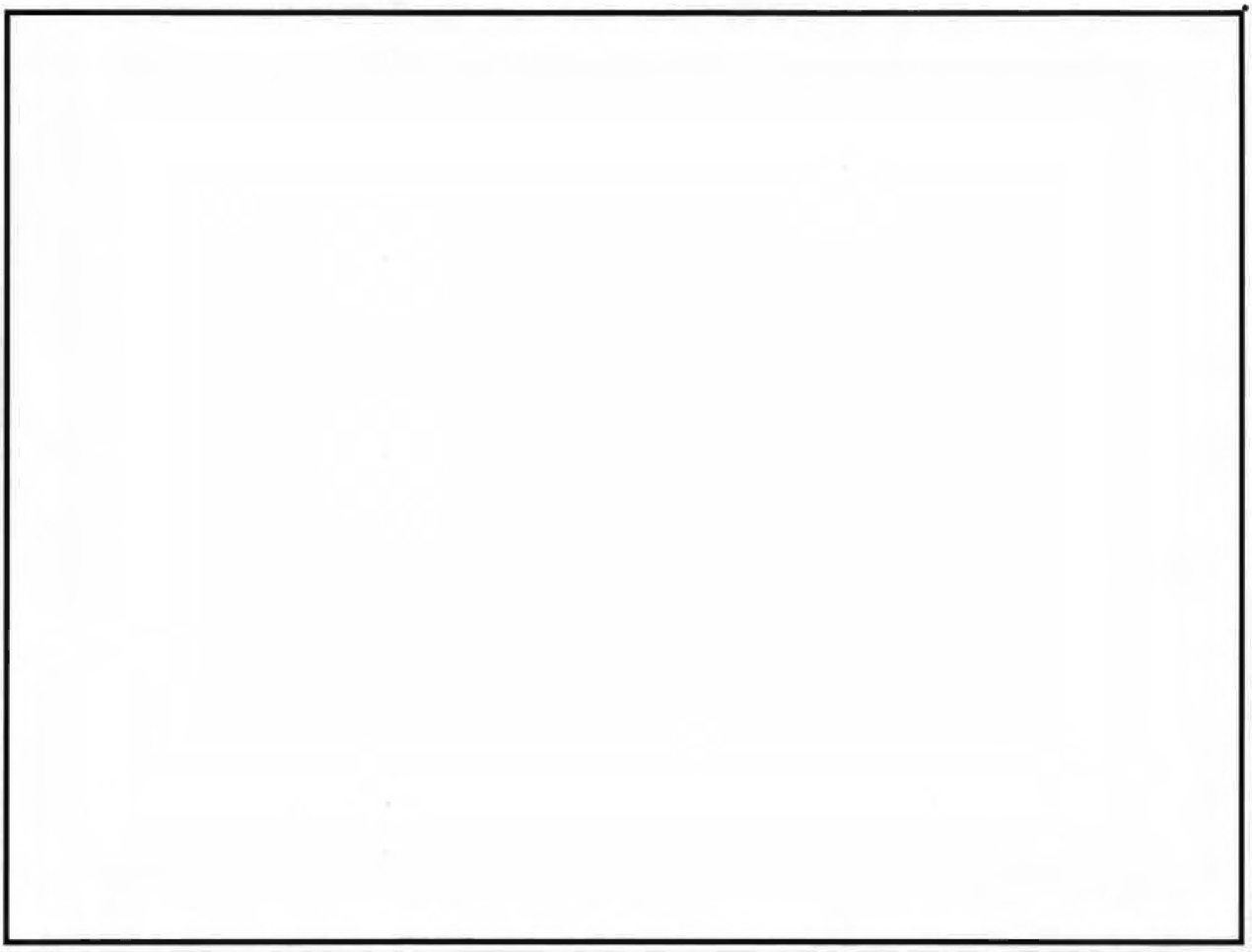
(b)(3)-P.L. 86-36

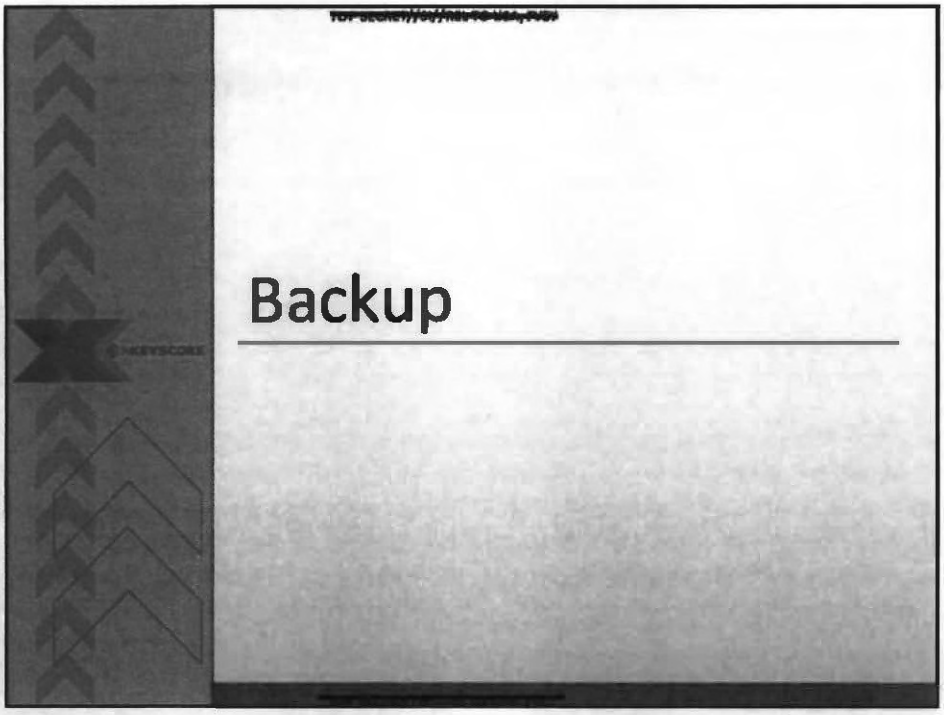




40






Backup

(b)(3)-P.L. 86-36