NSA-712 10 January 1955

STATUS OF [redacted] SYSTEMS
1954

This report includes all systems current on 31 December 1954 and all systems under study in NSA-712 at any time during the calendar year 1954.

DISTRIBUTION:

External - 20 copies
NSA-712 - 15 copies
NSA-7121 - 1 copy
NSA-7122 - 1 copy
NSA-7123 - 1 copy

INTRODUCTION

The two principal targets of NSA-712 during 1954 were the Diplomatic and Military problems. There are about [redacted] persons assigned to the Diplomatic problem and about [redacted] to the Military.

The most significant developments during the past year were as follows:

1. An attempt by the [redacted] to tighten up security in both Diplomatic and Military cryptographic systems. This trend reached its peak in June and July after which time security consciousness decreased somewhat.

2. The introduction of two voice scrambler systems in [redacted] the Single-Side-Band, 4-cycle AZ-13 and the Double-Single-Side-Band, 5-band system (the other side of which carries radio-printer traffic.

Generally speaking, the overall situation in NSA-712 during 1954 reflects conditions that have continued now for several years: inadequate numbers of cryptanalytic and linguistic personnel to carry out properly its mission. From a personnel strength of [redacted] in Jan 50 the Branch has been reduced to an average strength of about [redacted] people during 1954. This has been due, principally, to levies placed on Branch personnel to support higher-priority problems such as [redacted]. The inevitable cost to consumers has been fewer translations and a decrease in their timeliness. The intelligence yield to consumers represents only about [redacted] of its potential [redacted] Diplomatic and [redacted] Military.) In addition to this, the manning of extra shifts in response to special consumer priority requests, the establishment of a swing shift of arbitrary size, management surveys, periodic furniture reshuffling have all contributed to further limit the Branch's production.

PRODUCTION STATISTICS

	Oct-Dec 1954	Oct-Dec 1953	Year 1954	Year 1953	Year 1952
Orig Cipher Msgs Recd	51,551	34,238*	213,427	137,693*	102,896*
Dupe Cipher Msgs Recd	21,135	37,781	108,498	126,610	110,428
Total Cipher Msgs Recd	72,686	72,019*	321,925	264,303*	213,324*
Cipher Msgs Decrypted	21,030	19,568	87,908	82,566	59,163
Cipher Msgs Translated	4,730	4,556	20,137	21,743	21,570
Cipher Msgs Summarized	494	640	2,649	2,619	738
P/L Msgs Trans or Summ	590**	641	1,401**	2,040**	714**
Code Meanings Recovered	2,363	5,554	14,252	15,544	22,561
Aver Number Personnel	118	130	122	129	122

INTERCEPT/TRAFFIC ANALYSIS

Although the Production Statistics indicate that the volume of original messages received for 1954 is about the same as it was for 1953, there has been a downward trend in receipts since June. The loss of a large volume of [redacted] traffic (B-211 machine encipherment of high-level military traffic) between May and August as a result of a change from Morse and Teletype transmission to Double Single Side Band was a major factor in this decrease. Although USM-9 began to intercept [redacted] on the DSSB in August, the traffic volume remains low because difficulty has been experienced in acquiring all the equipment necessary to intercept this new type of transmission and because of the loss of [redacted] and the consequent decrease in the amount of traffic sent by the [redacted].

In 1953, it was estimated that [redacted] cipher traffic received was passed on the [redacted] These percentages have not changed much for 1954, except that there has been some increase in radio-printer traffic as a result of the installation of the [redacted] in October 1953 and a corresponding decrease in [redacted] Net traffic.

* 1952 and 1953 figures for cipher messages do not include a large number of unsolved [redacted] messages, the volume of which is estimated to be [redacted] per month.

** Plain-language messages received are not counted. It is estimated that about [redacted] are received and scanned quarterly. Plain-language messages used in reports are included in these figures.

From the standpoint of exploitability and consumer interest, the importance of [redacted] net traffic cannot be too highly stressed. Intercept receipts have remained fairly steady for this year with about [redacted] of the total sent being successfully intercepted compared with [redacted] in 1953. The recent loss of [redacted] traffic both in quality and quantity - is regrettable and it is hoped that it will not cause too great harm to the [redacted] problem.

This loss, in addition to the complete loss of cover at Station USN-18 during the year, made it seem essential to provide for [redacted] cover to the extent of 3 positions located on the continent. NSA-712 was successful in having one position at STATION USM-6 assigned to this problem at the end of November with very favorable results based on one month's take.

A new attempt is being made at Station USM-6 to intercept [redacted] traffic passing between [redacted] which is thought to be sent by means of the "True-Tone" system. Since both [redacted] and the Air Force are interested in this traffic, it is hoped that all possible effort will be made this time to obtain the proper equipment and personnel to intercept this traffic which NSA-712 has desired for so long.

During the last half of 1954 the AZ-13 and the 5-band voice scramblers came into general use. Shortly after the fall of [redacted] Hanoi started using the AZ-13 almost exclusively although the hand-morse and teleprinter circuits were kept open. This caused a drop of about [redacted] traffic.

In July the second voice scrambler (5-band) in use in [redacted] was identified. It is passed on one side of a Double Single Side Band system, the other side of which was found to carry the [redacted] traffic which had been missing since May 54. USM-9 is now intercepting some of the traffic passed in these systems. However, lack of proper equipment has prevented full interception and exploitation of the two scrambler systems and the DSSB. The partial intercept of the Double Single Side Band transmissions restored some of the [redacted] traffic but the volume is still far below normal.

CRYPTANALYTIC DEVELOPMENTS

I. [redacted] MACHINE SYSTEMS

The readability of this [redacted] in 1954.* Difficulties encountered in solution were the lack of workable depths as a result of [redacted]

* See Attachment A.

There were several important highlights in solution during the year.

[redacted]

1) Electrical forwarding of USM-8ØE traffic by NSA-13.

2) Special processing at both ends of NSA-13's circuits. Among other things, this involved a [redacted]

3) A special Courier forwarding arrangement which cut the average delivery time of hard copy from 7 to 1½ days.

[redacted]

Solution of these systems has progressed slowly since the

Little is known about this series.

However, it is felt that more groups are involved in each of the indicator systems, although recent studies, including a have not revealed them.

Most of the solution work on , the assumed predecessor of the series, was accomplished during the first few months of 1954. When work was abandoned .

3. The

Solution and exploitation of this series of

In August, the

4. A small effort was directed during the year to [redacted] which is used, for the most part, during conferences, and to [redacted] which started during the [redacted] lanes and is slowly dying out. It is believed that these systems use one-time pads.

III. [redacted]

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

RESEARCH AND MACHINE AIDS

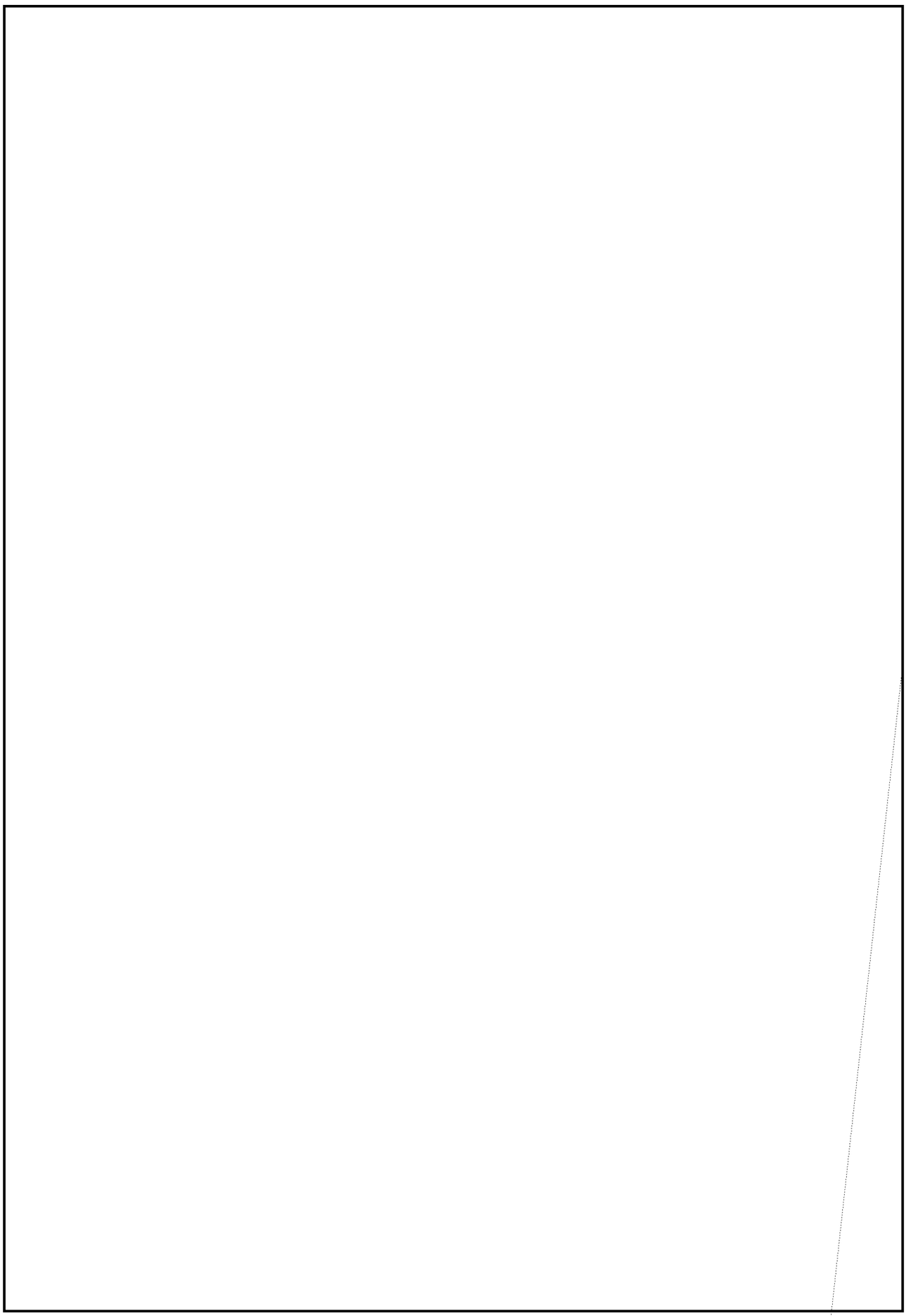
1. Computer Programs

The following computer programs were designed for use on ATLAS II.

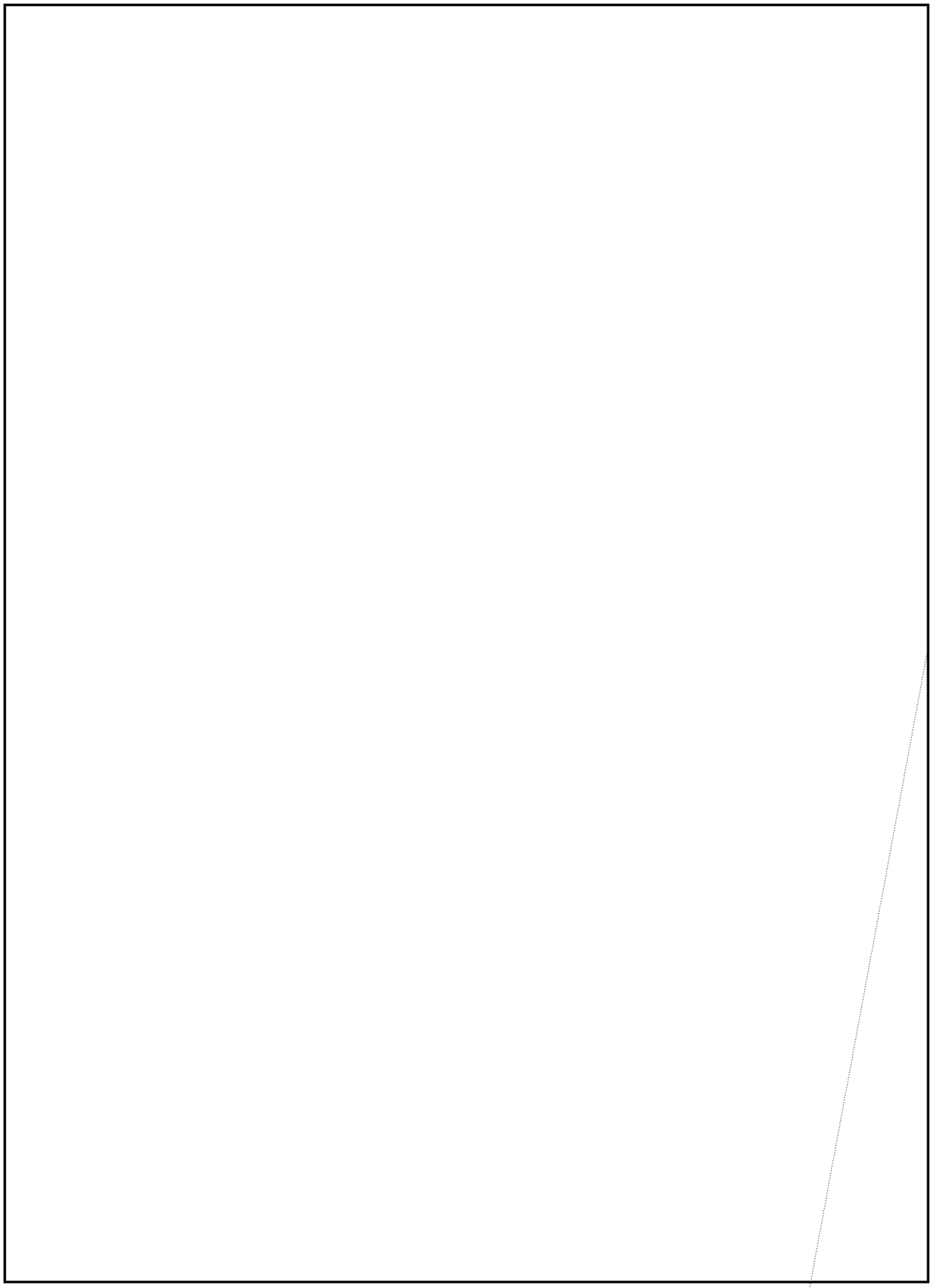
2. Machines

INTELLIGENCE PRODUCTION

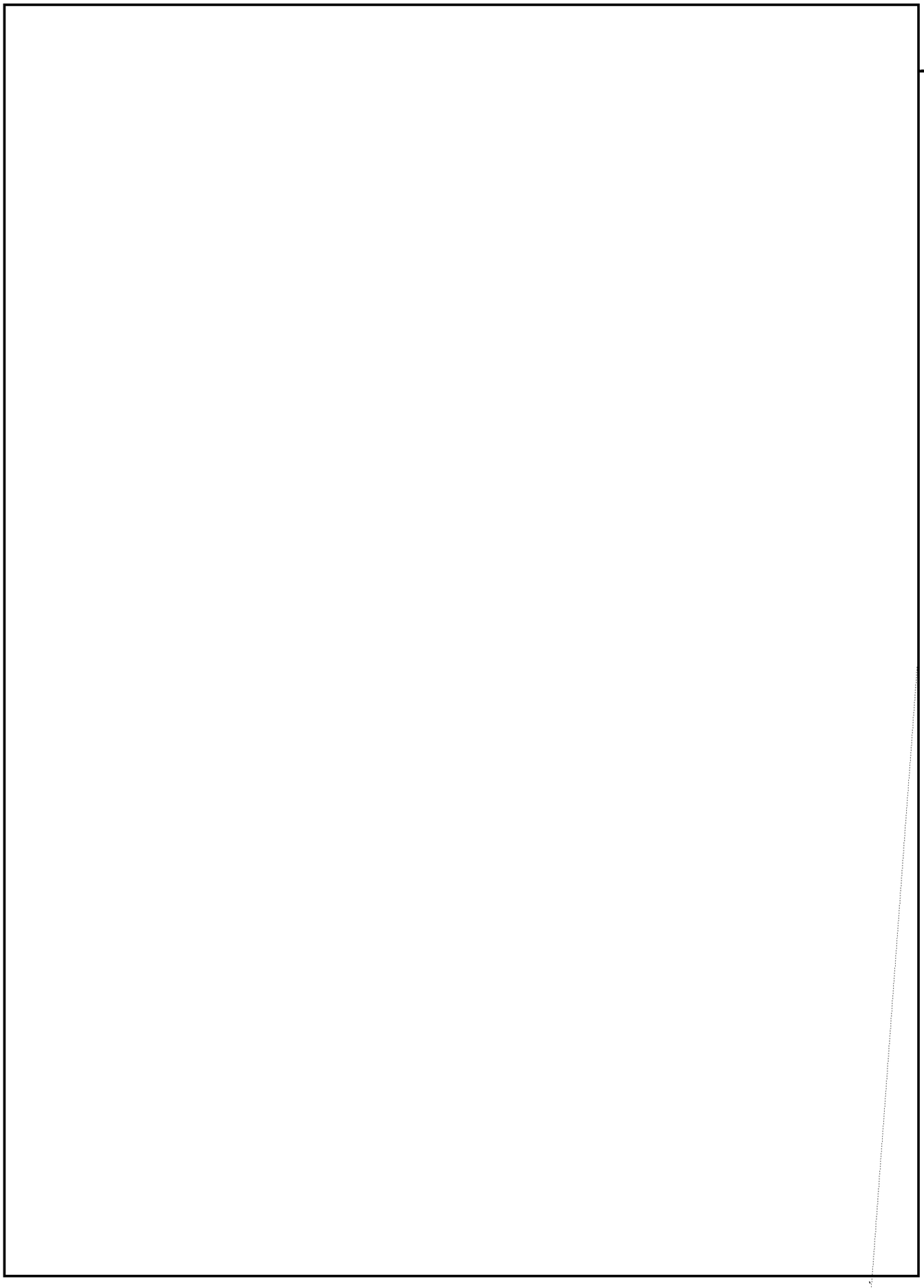
From the Production Statistics it will be noticed that

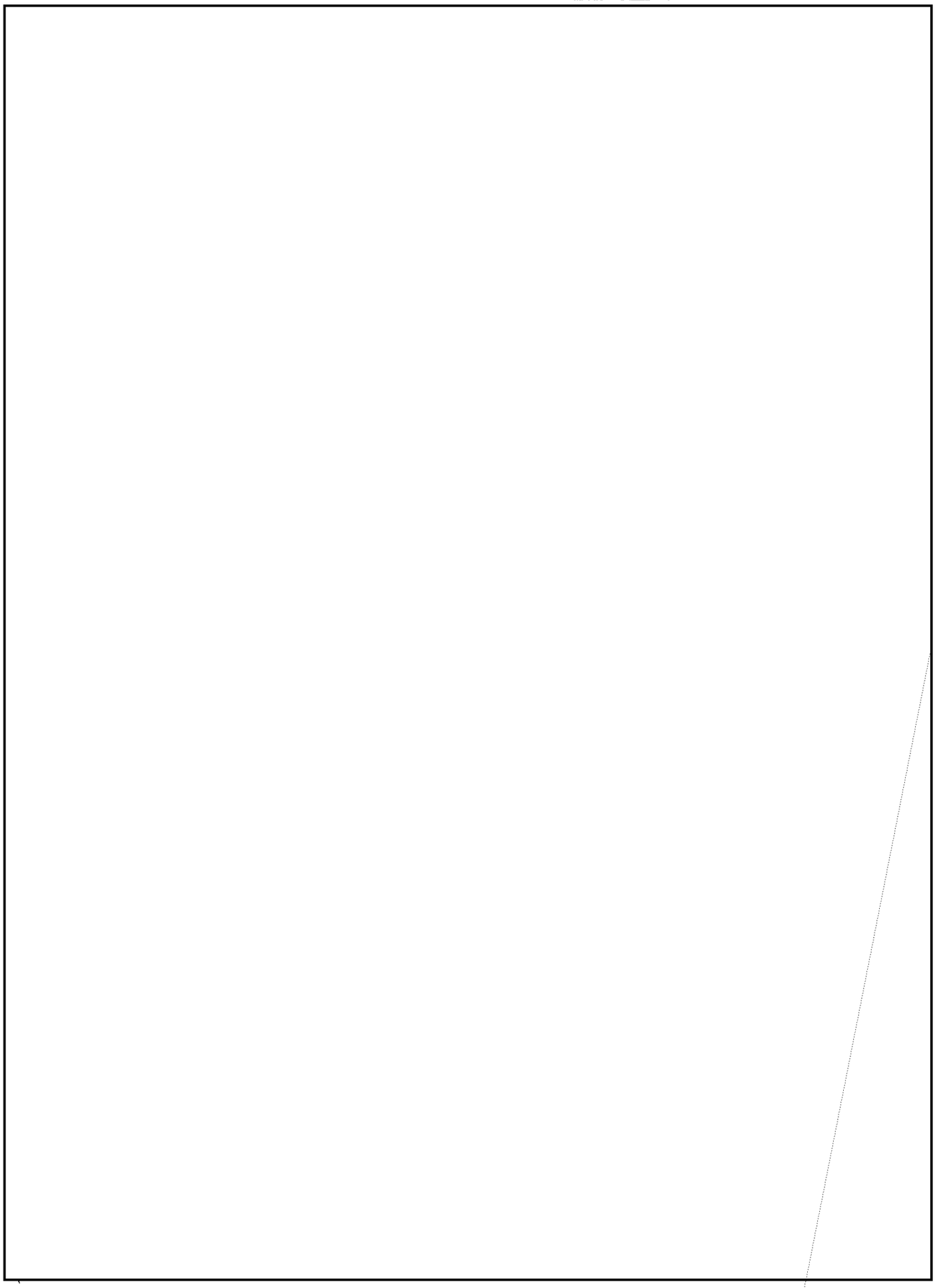


PL 86-36/50 USC
EO 3.3(h)(2)

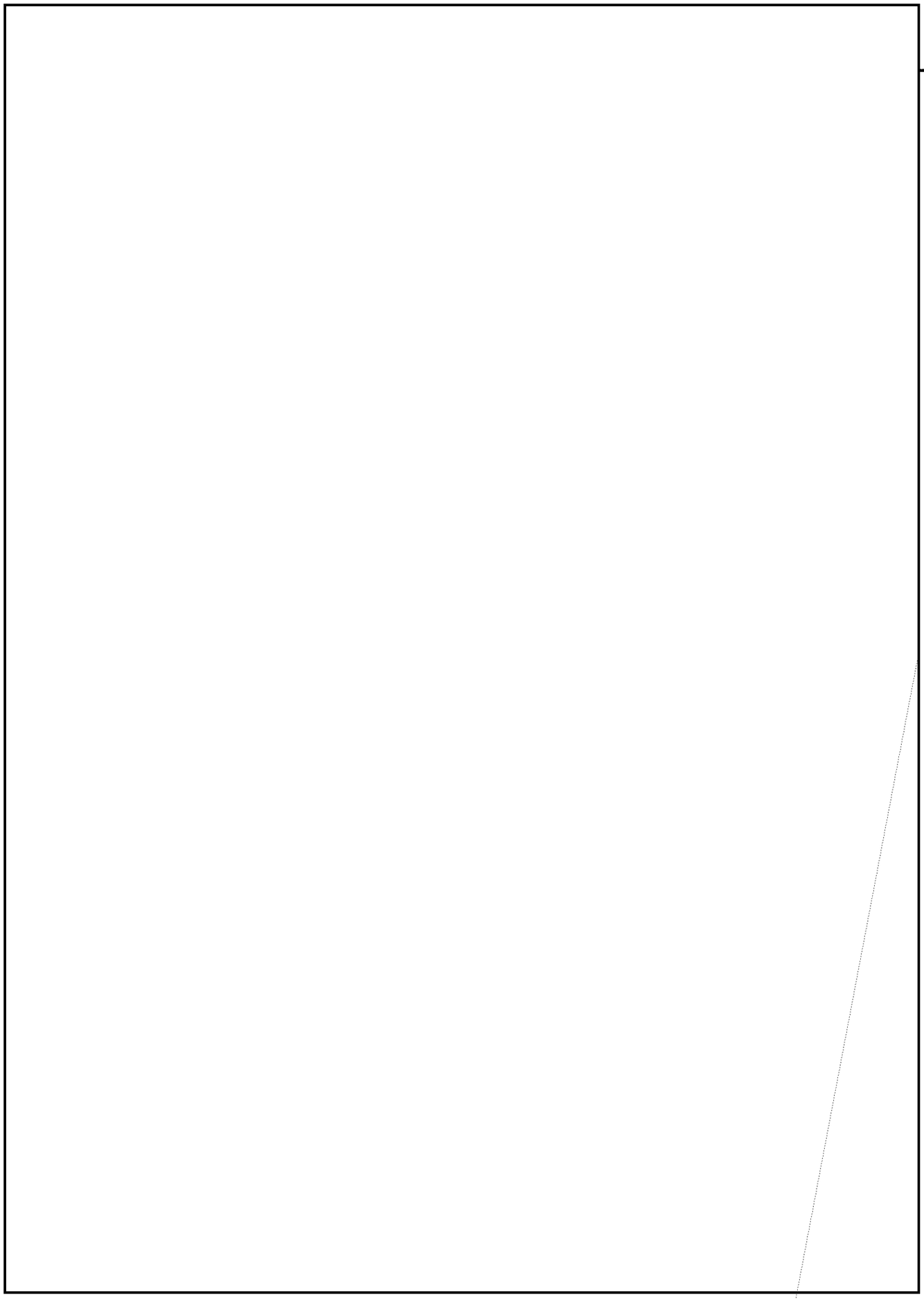


PL 86-36/50 USC 3605
EO 3.3(h)(2)

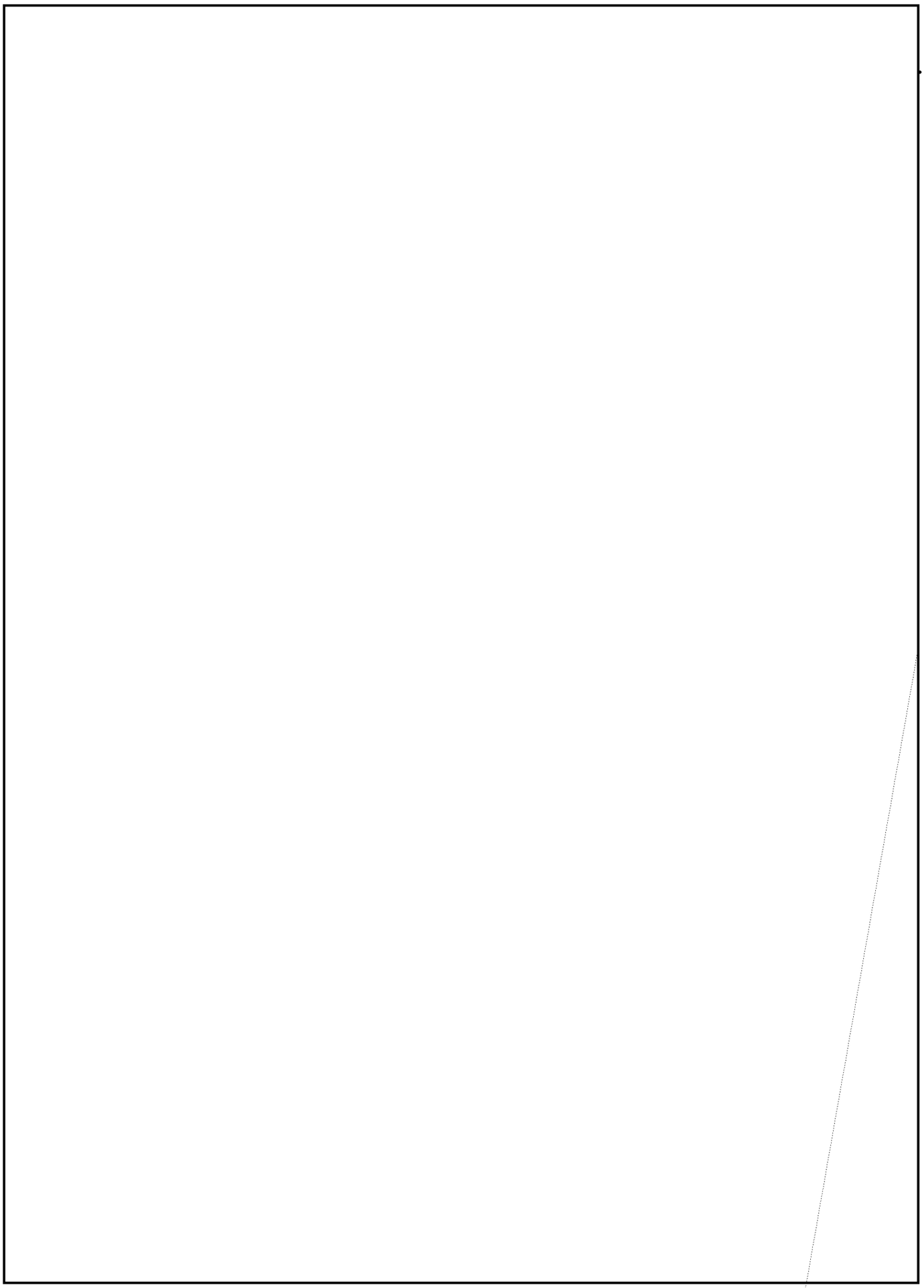


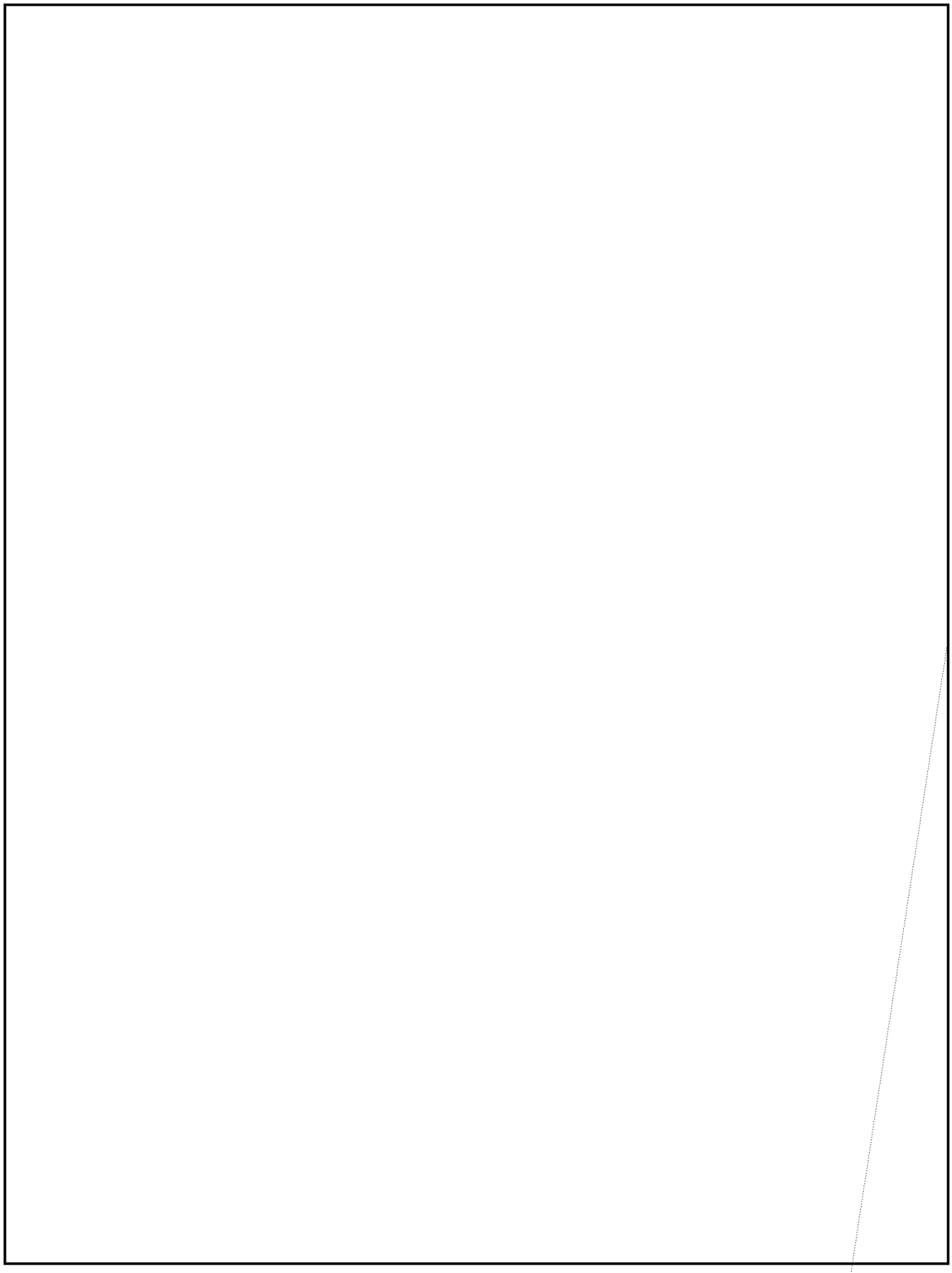


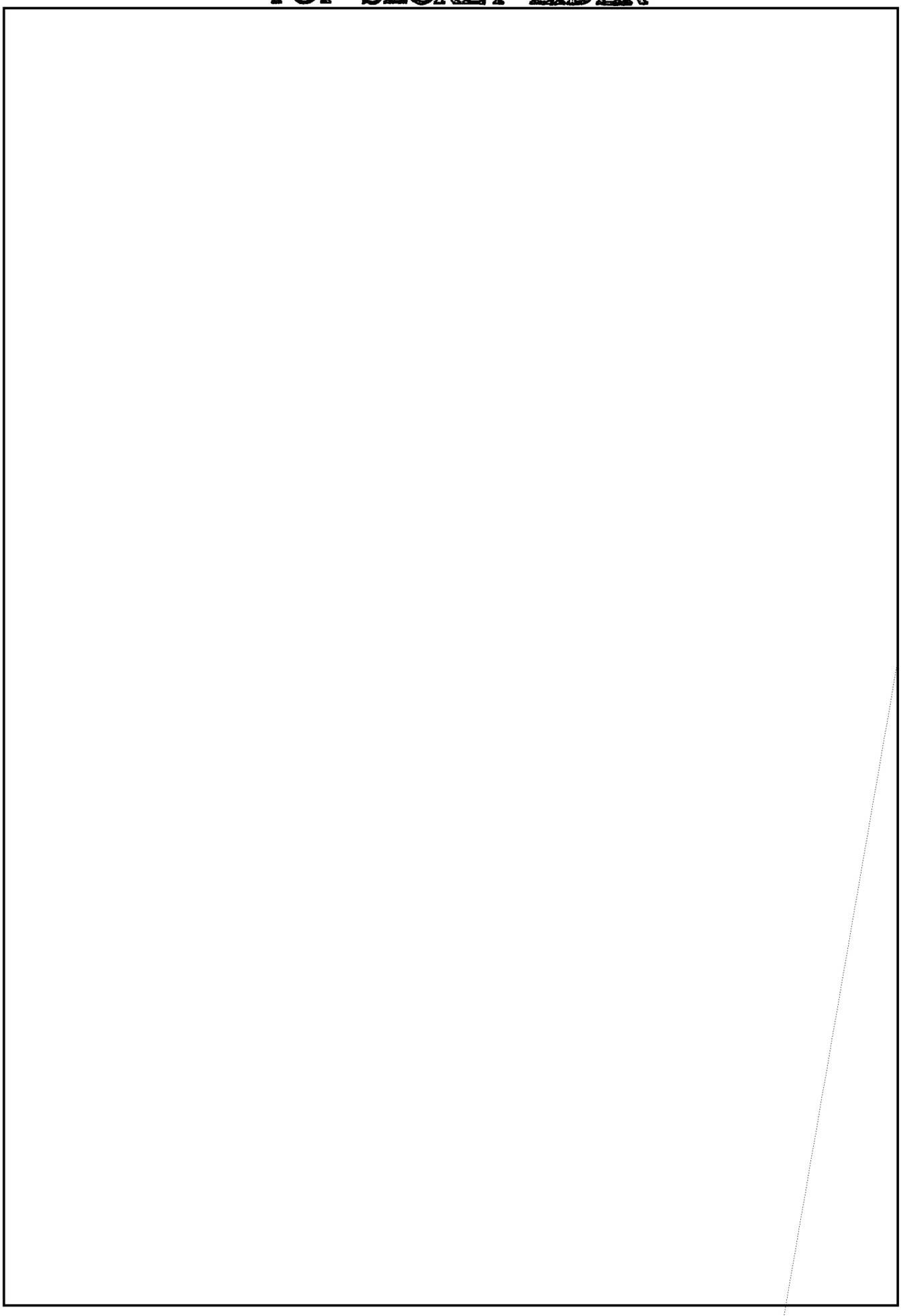
PL 86-36/50 USC 3605
EO 3.3(h)(2)

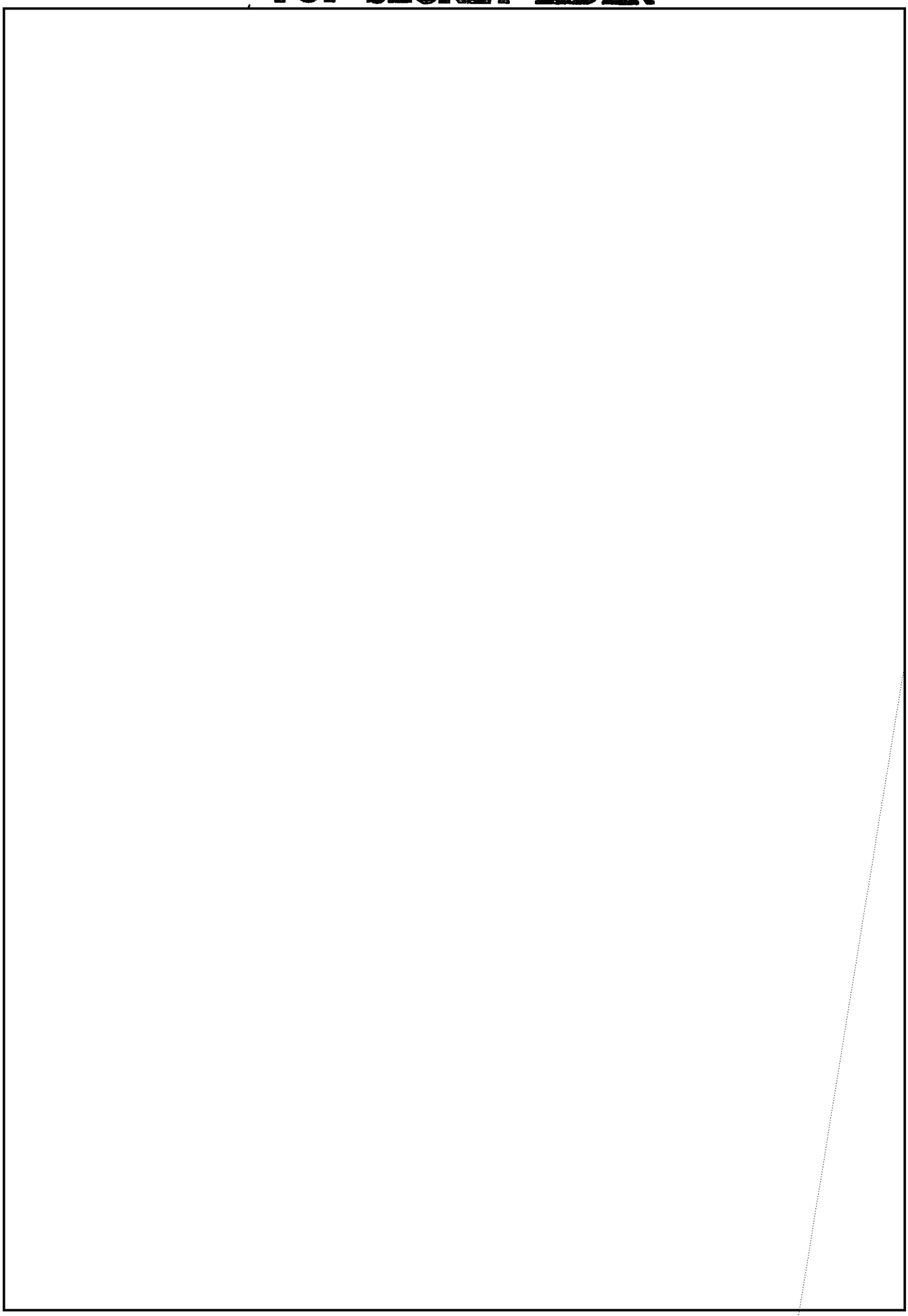


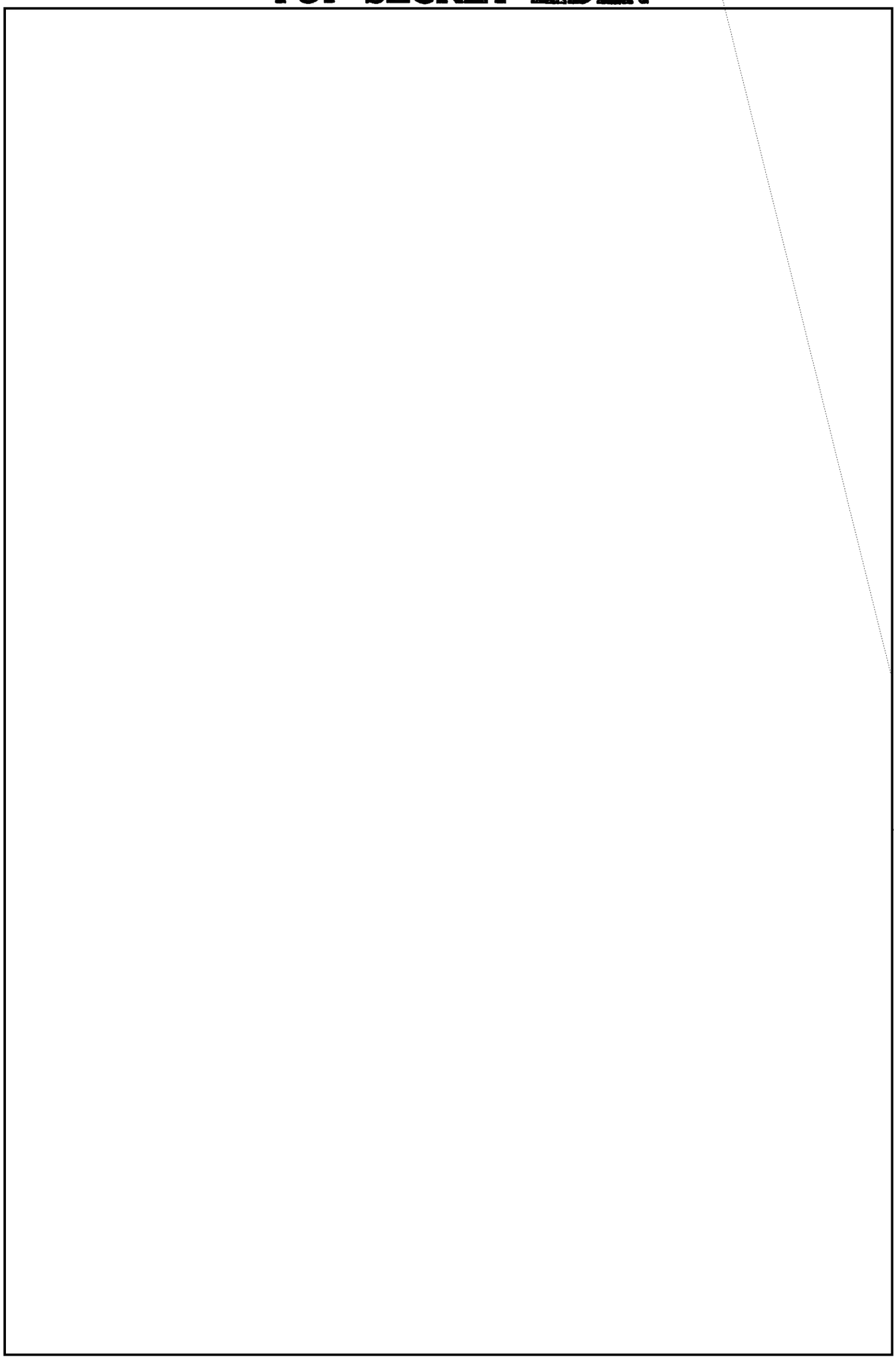
PL 86-36/50 USC 3605
EO 3.3(h)(2)

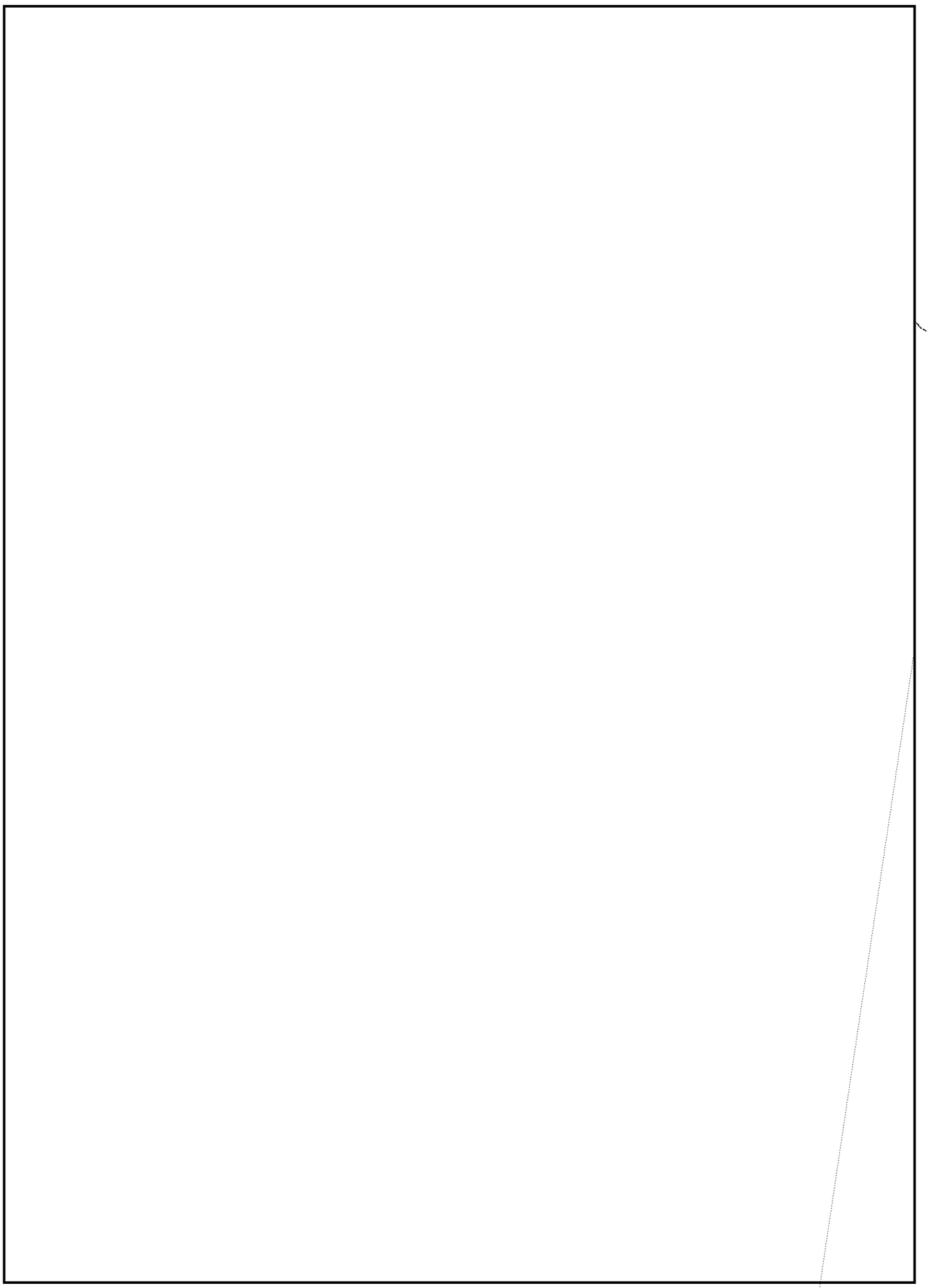




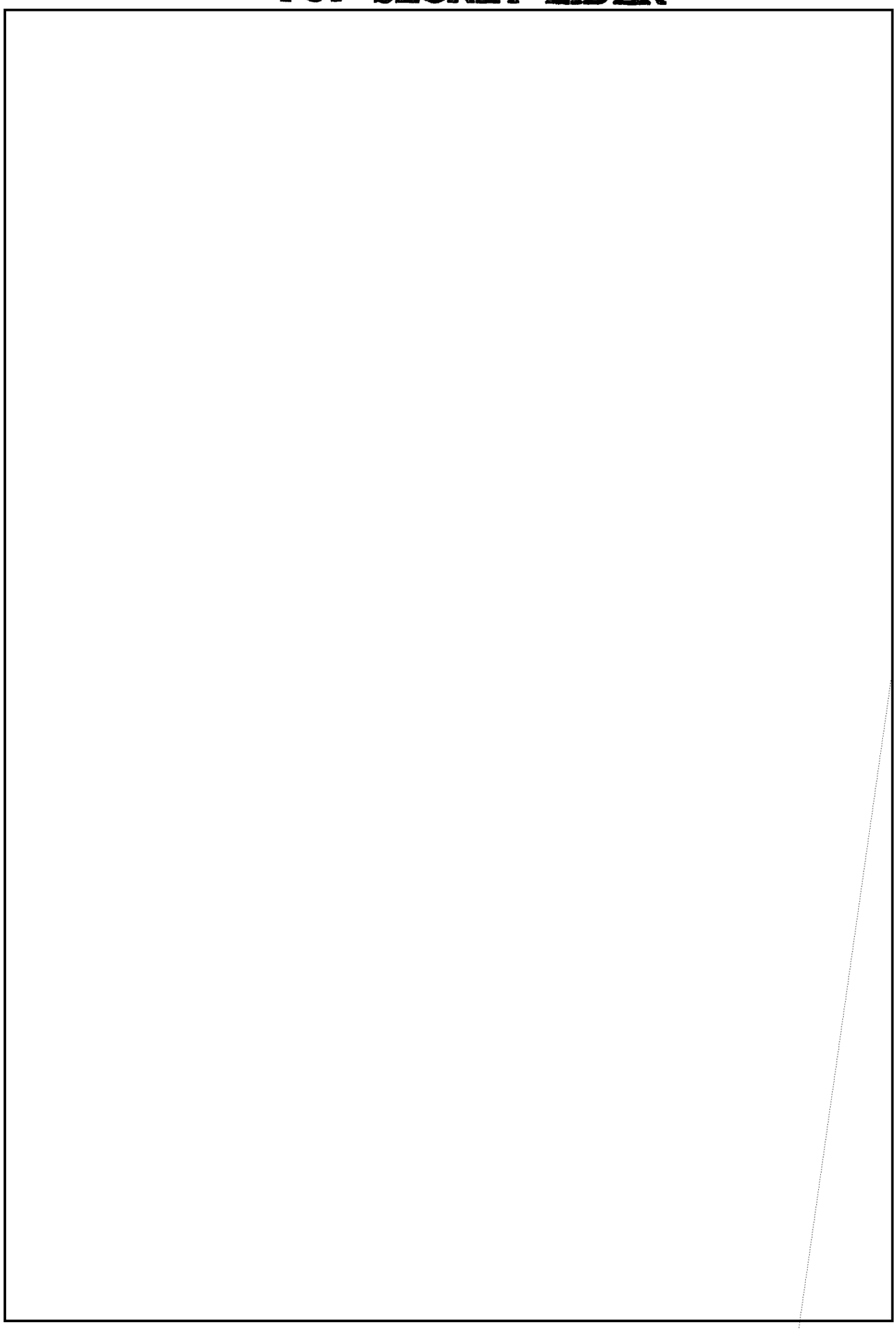


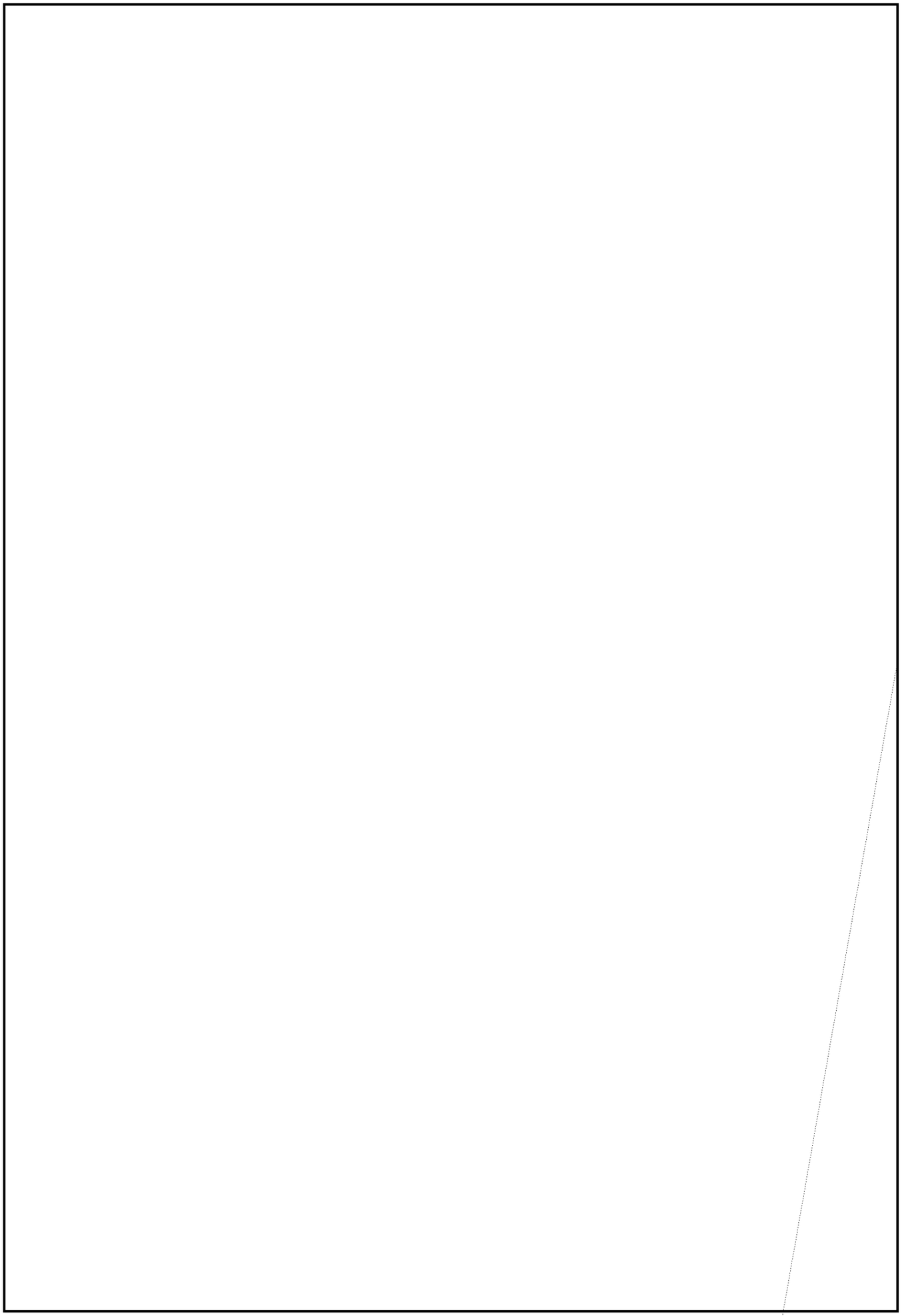


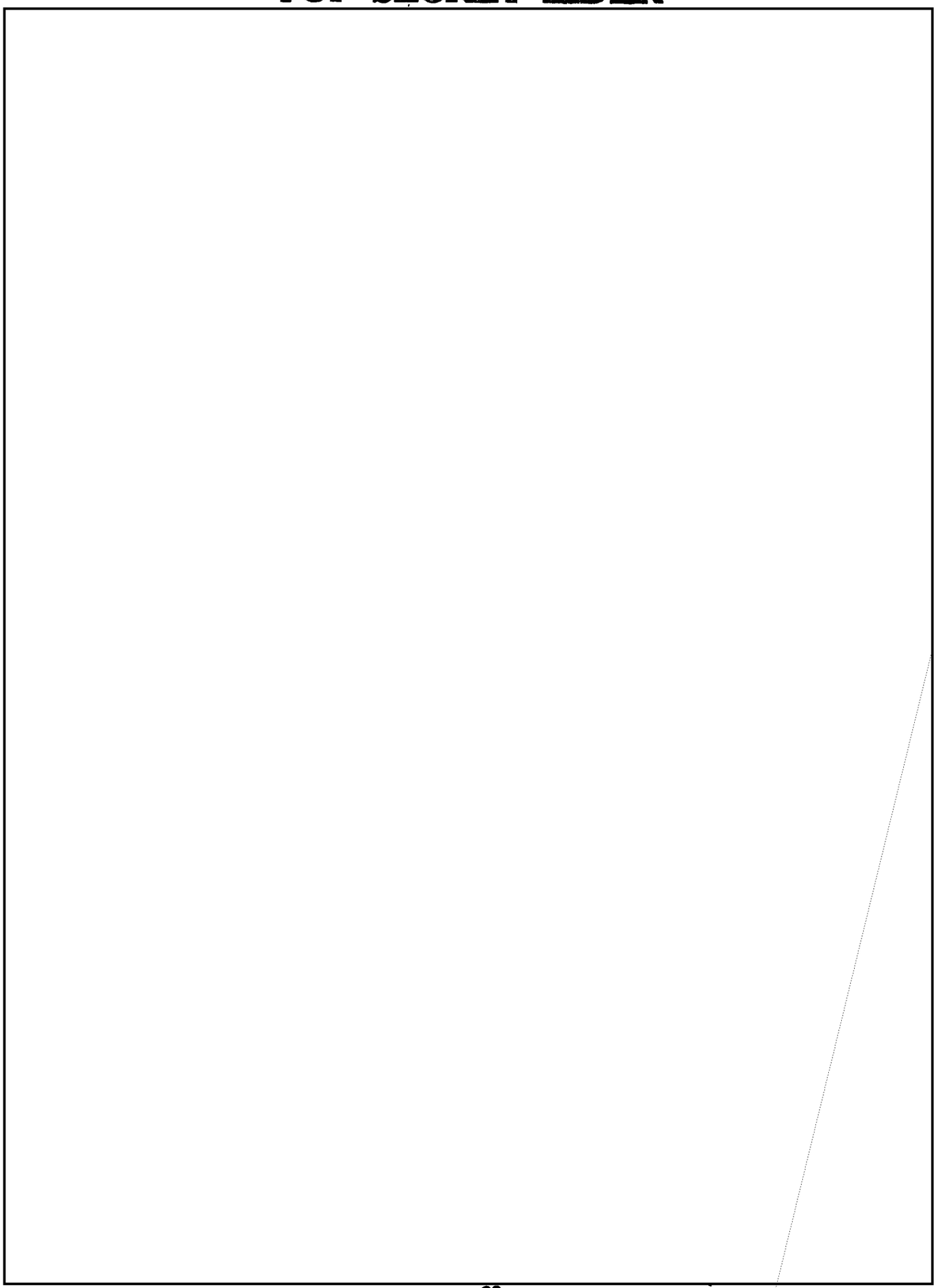




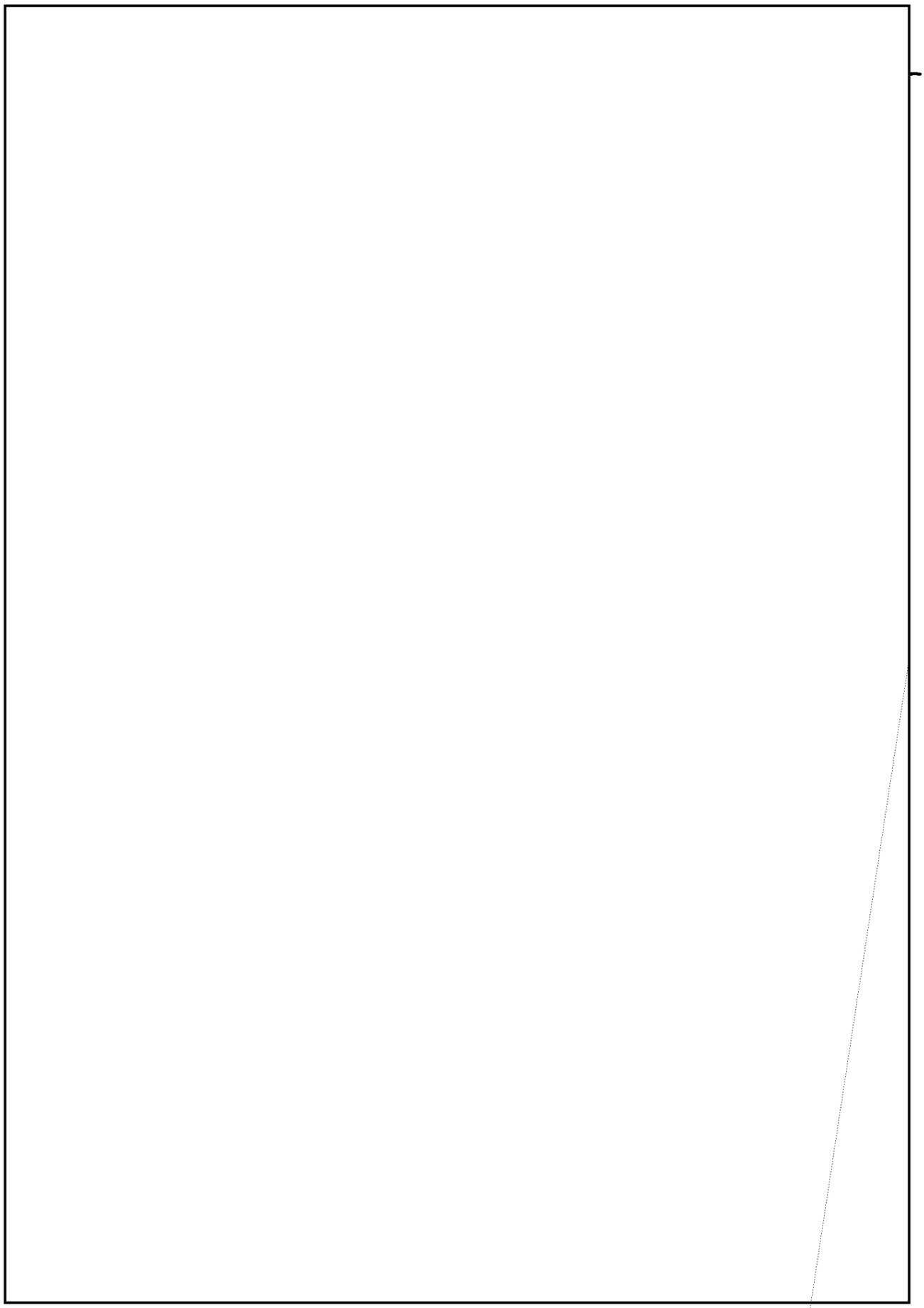
PL 86-36/50 USC 360
EO 3.3(h)(2)

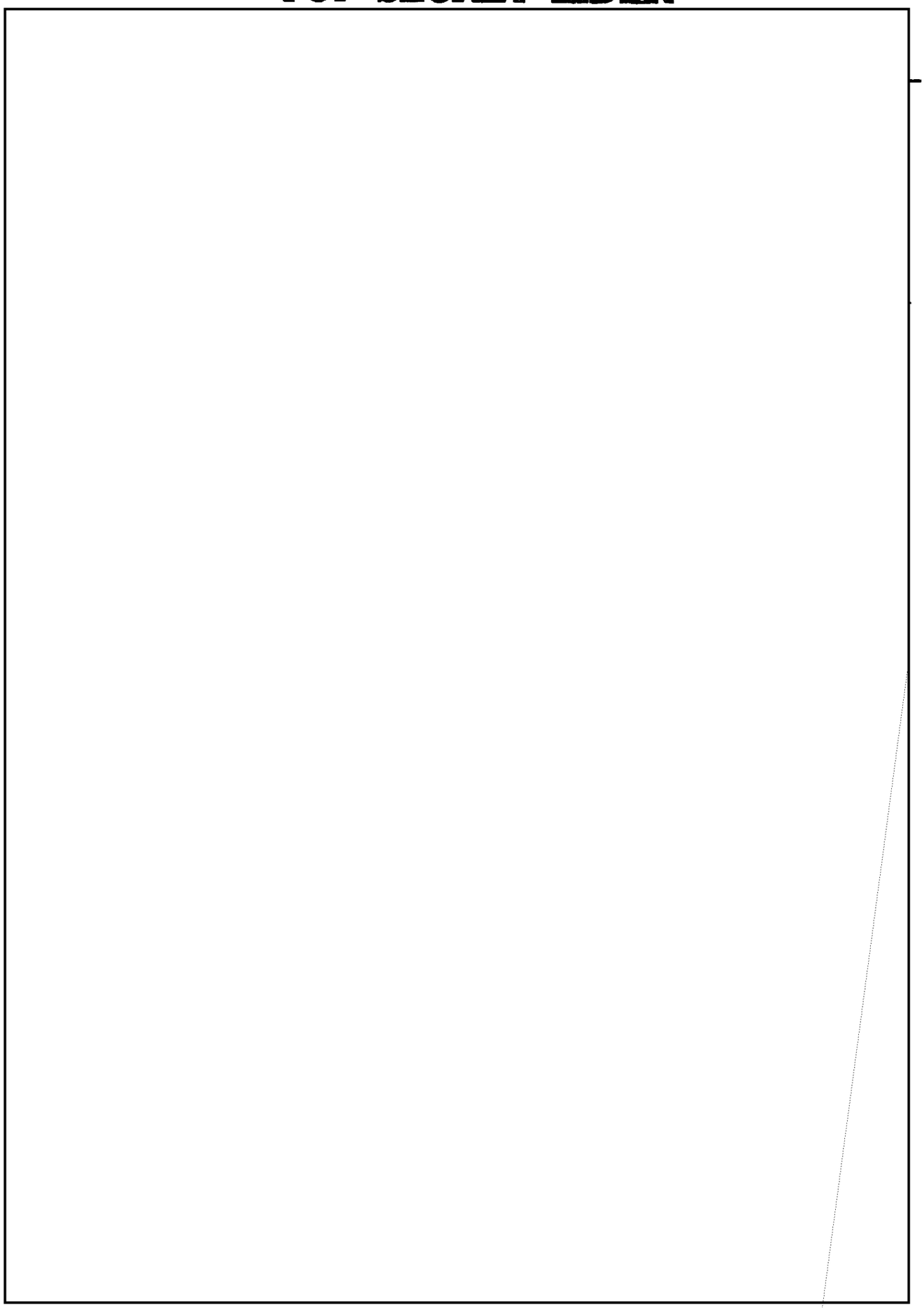


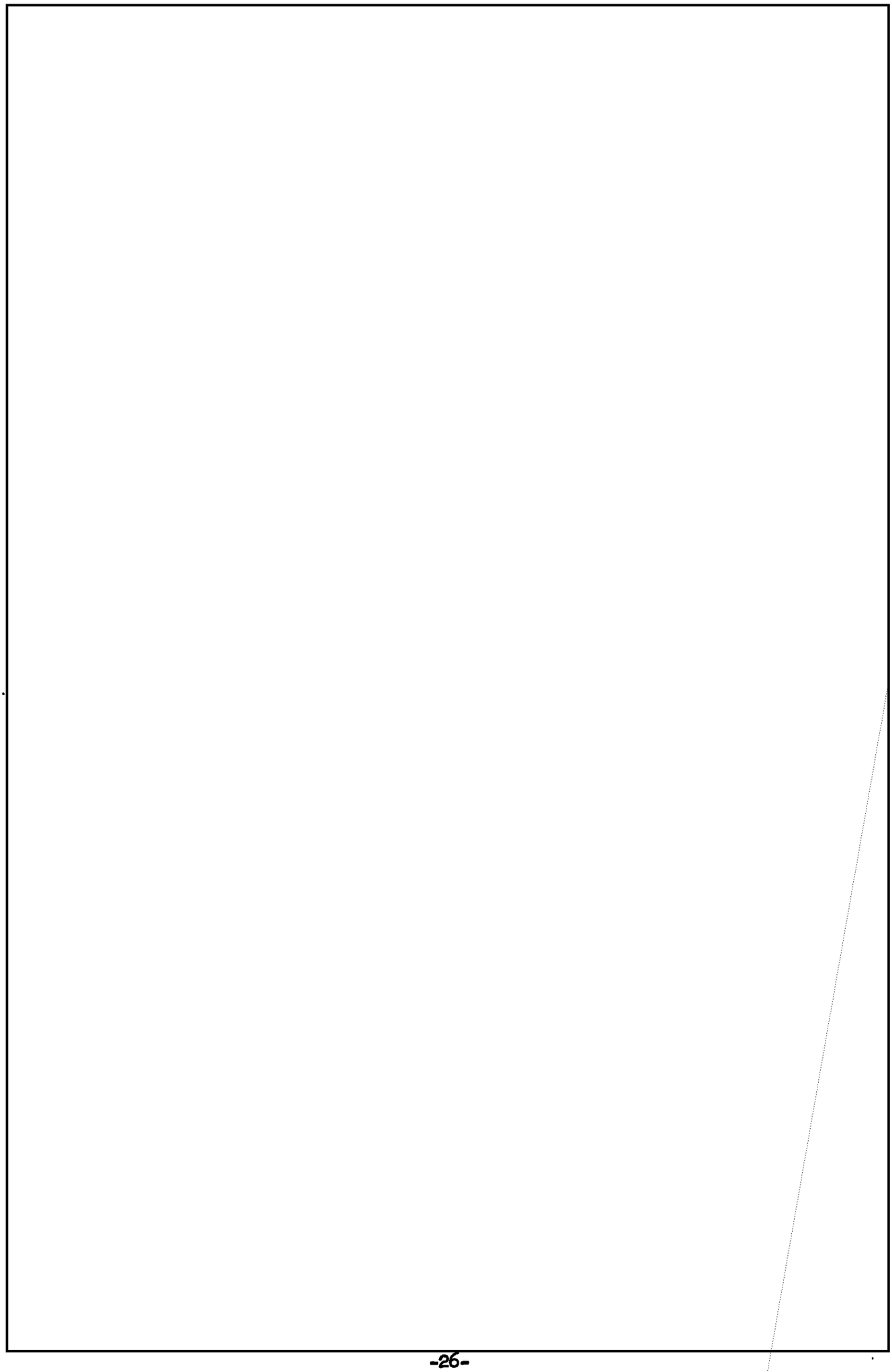


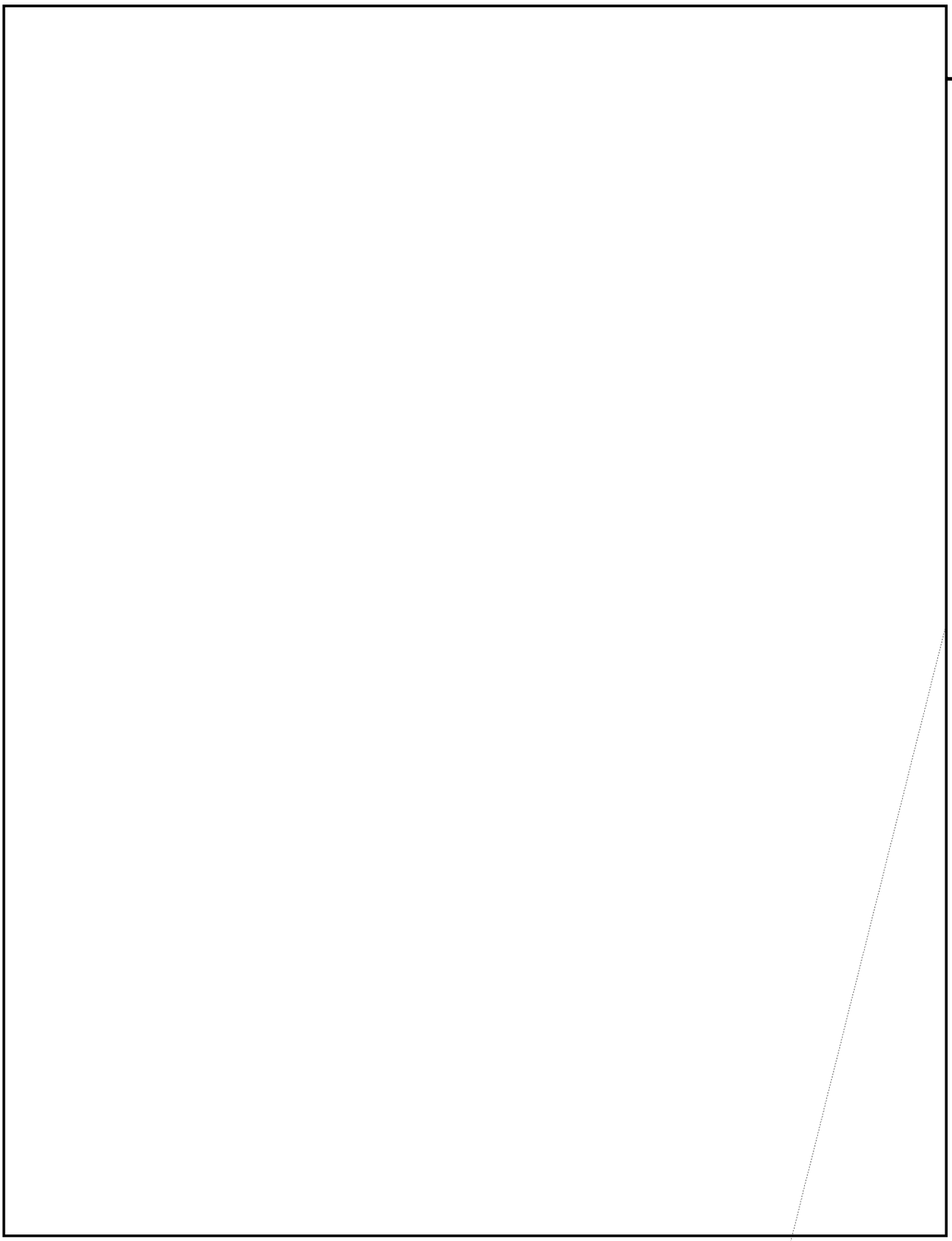


PL 86-36/50 USC 3605
EO 3.3(h)(2)









PL 86-36/50 USC 3605
EO 3.3(h)(2)

ATTACHMENT A

TOP SECRET EIDER

Jan.	1,834	5ø	51ø	11	386	25	245	9	1,749	15	1,413	16	1,732	1ø4	7,869	23ø
Feb.	1,625	38	452	21	384	148	142	4ø	982	4	882	1ø	2,7ø2	15ø	7,169	411
Mar.	1,616	124	449	44	475	13ø	3øø	64	1,263	5	1,326	11	2,538	75	7,967	453
Apr.	1,598	1ø7	472	61	575	13ø	325	92	1,377	8	1,152	12	2,329	74	7,828	484
May	1,459	134	4ø5	9	227	34	142	25	1,38ø	9	753	25	1,714	74	6,ø8ø	31ø
Jun.	1,19ø	3	333	5	323	1ø	2ø1	1	1,296	ø	814	1	1,352	8	5,5ø9	28
Jul.	1,ø45	2ø	290	5	21ø	ø	131	3	1,242	ø	1,023	ø	1,849	19	5,79ø	47
Aug.	1,ø34	ø	288	8	232	45	144	19	9ø6	9	843	ø	1,464	5	4,911	86
Sep.	1,382	1	385	36	233	ø	145	7	1,377	3	864	ø	2,1ø0	13	6,486	6ø
Oct.	1,543	27	428	36	18ø	2	111	2ø	1,6ø8	16	1,398	2	2,611	61	7,879	164
Nov.	1,8ø9	71	5ø3	18	237	ø	148	13	1,98ø	13	1,854	16	2,545	245	9,ø76	376
Dec.	1,591	41	441	14	168	1ø	1ø8	9	1,554	ø	1,476	4	2,285	66	7,623	144
Total	17,726	616	4,956	268	3,63ø	534	2,142	3ø2	16,714	82	13,798	97	25,221	894	84,187	2,793 (3.3%)