

~~TOP SECRET~~

REF ID: A58758 *Hagelin Telecrypto 4-13-1*

~~SECURITY INFORMATION~~

Office Memorandum • UNITED STATES GOVERNMENT

TO OOT ←

DATE 23 Jan 52

FROM 412

SUBJECT Forwarding of Report

*File
Hagelin
Telecrypto*

The following report is forwarded for your information and retention:

AFSA-412E2-1550.2, "Recognition of All Machine Variables From Two Messages 1000 Characters in Length on Telecrypto With One Cylinder Offset Between the Messages".



R. H. SHAW
Head, AFSA-412

Declassified and approved for release by NSA on 07-11-2014 pursuant to E.O. 13526

~~TOP SECRET~~

~~TOP SECRET~~

REF ID:A58738

~~TOP SECRET SECURITY INFORMATION~~

AFSA-412B2-1550.2
6 November 1951

RECONSTRUCTION OF ALL MACHINE VARIABLES FROM TWO MESSAGES, 1000 CHARACTERS IN LENGTH ON TELECRYPTO WITH ONE CYLINDER OFFSET BETWEEN THE MESSAGES

I. Summary

1. References:

- a. Letter from B. Hagelin to Mr. W. F. Friedman, dated 21 May 51.
- b. AFSA-412B Memorandum, "Brief Security Estimate of Telecrypto", dated 15 June 51.
- c. AFSA-412B2-1550.1.

2. Purpose: To reconstruct all machine variables.

3. Given:

a. Two messages, 1000 characters in length enciphered on Telecrypto. Settings of all variables are the same for both messages, except for the setting of one cylinder.

b. Knowledge of the machine, including the location of the fixed stepping teeth on the drum.

4. Results:

- a. The two messages are read and key recovered.
- b. All machine variables are reconstructed.

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

5. Remarks:

~~TOP SECRET~~

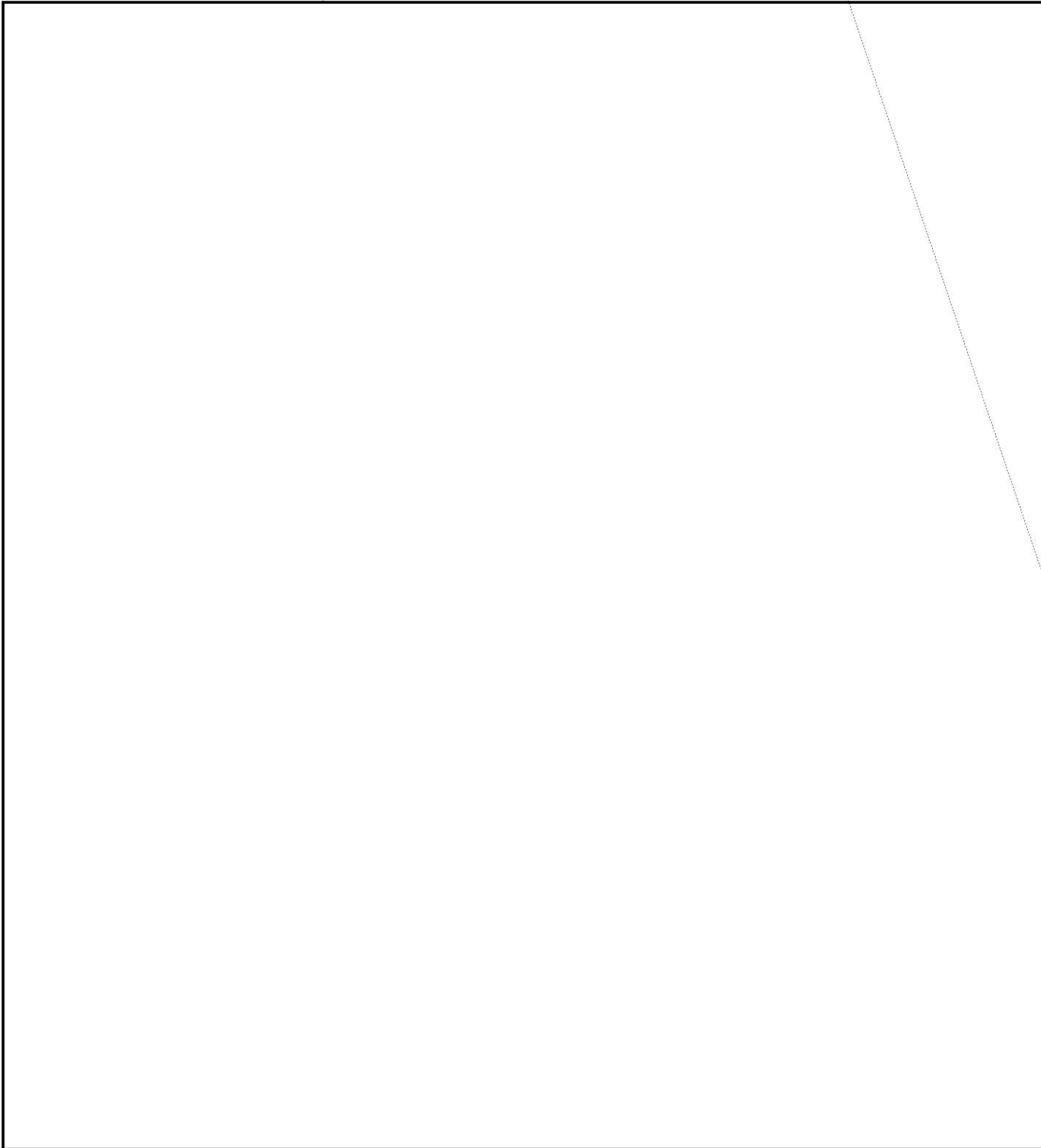
~~TOP SECRET~~

REF ID: A58738

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

~~TOP SECRET SECURITY INFORMATION~~

II. Solution



~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A58738

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

~~TOP SECRET SECURITY INFORMATION~~



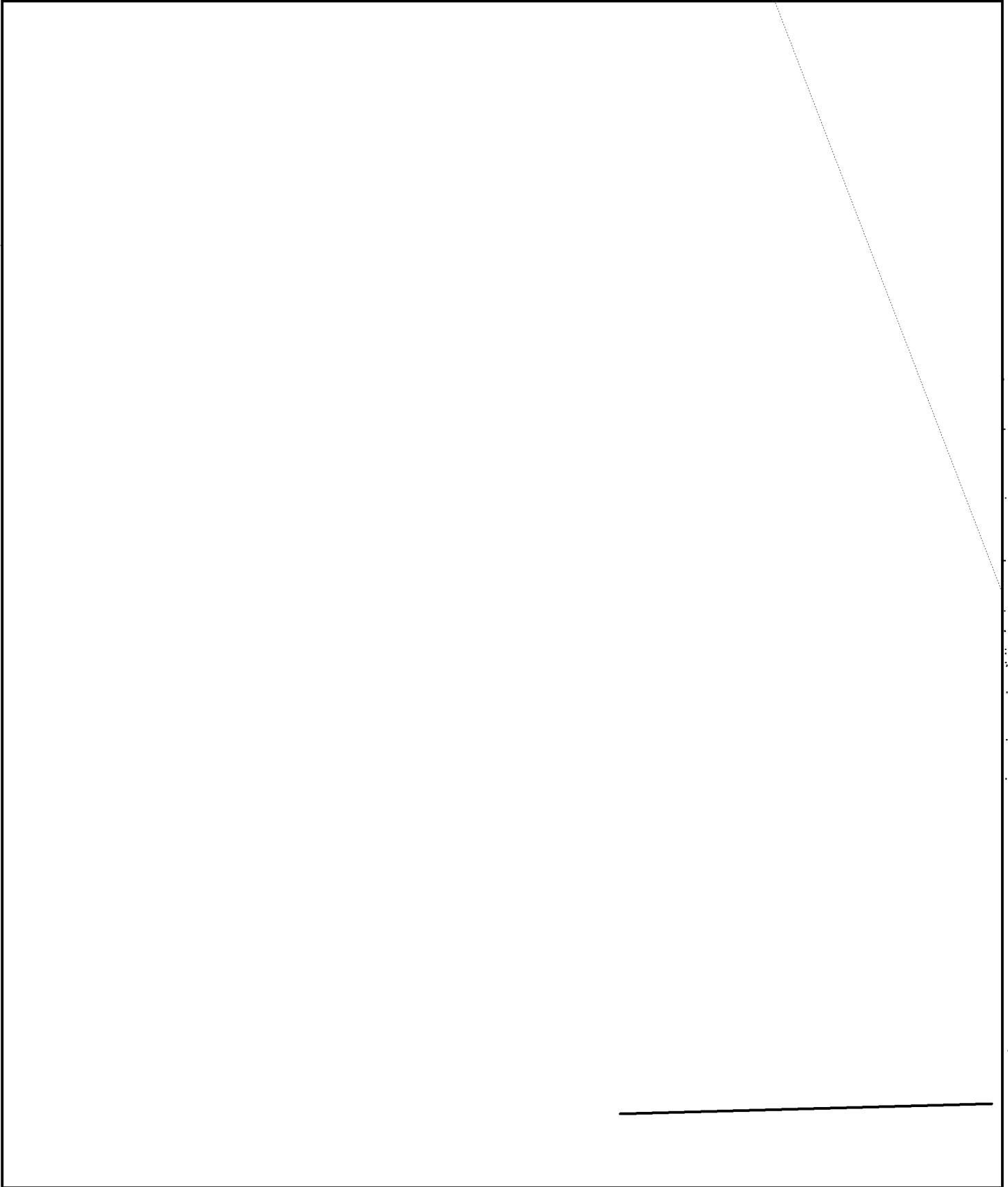
~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A58738

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

~~TOP SECRET SECURITY INFORMATION~~

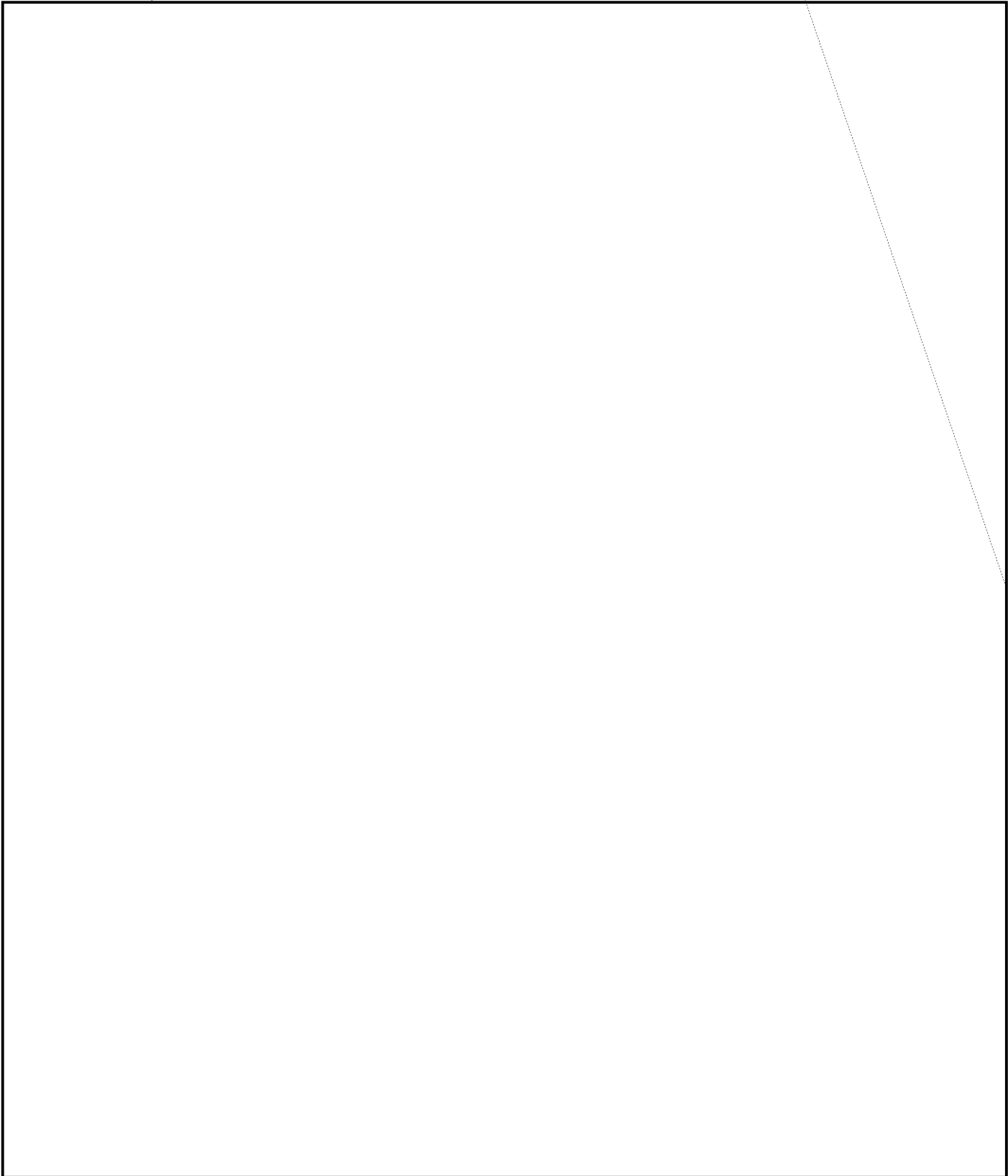


~~TOP SECRET~~

REF ID: A58738

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

~~TOP SECRET SECURITY INFORMATION~~



~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A58738

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

~~TOP SECRET SECURITY INFORMATION~~

ANALYSIS BY:

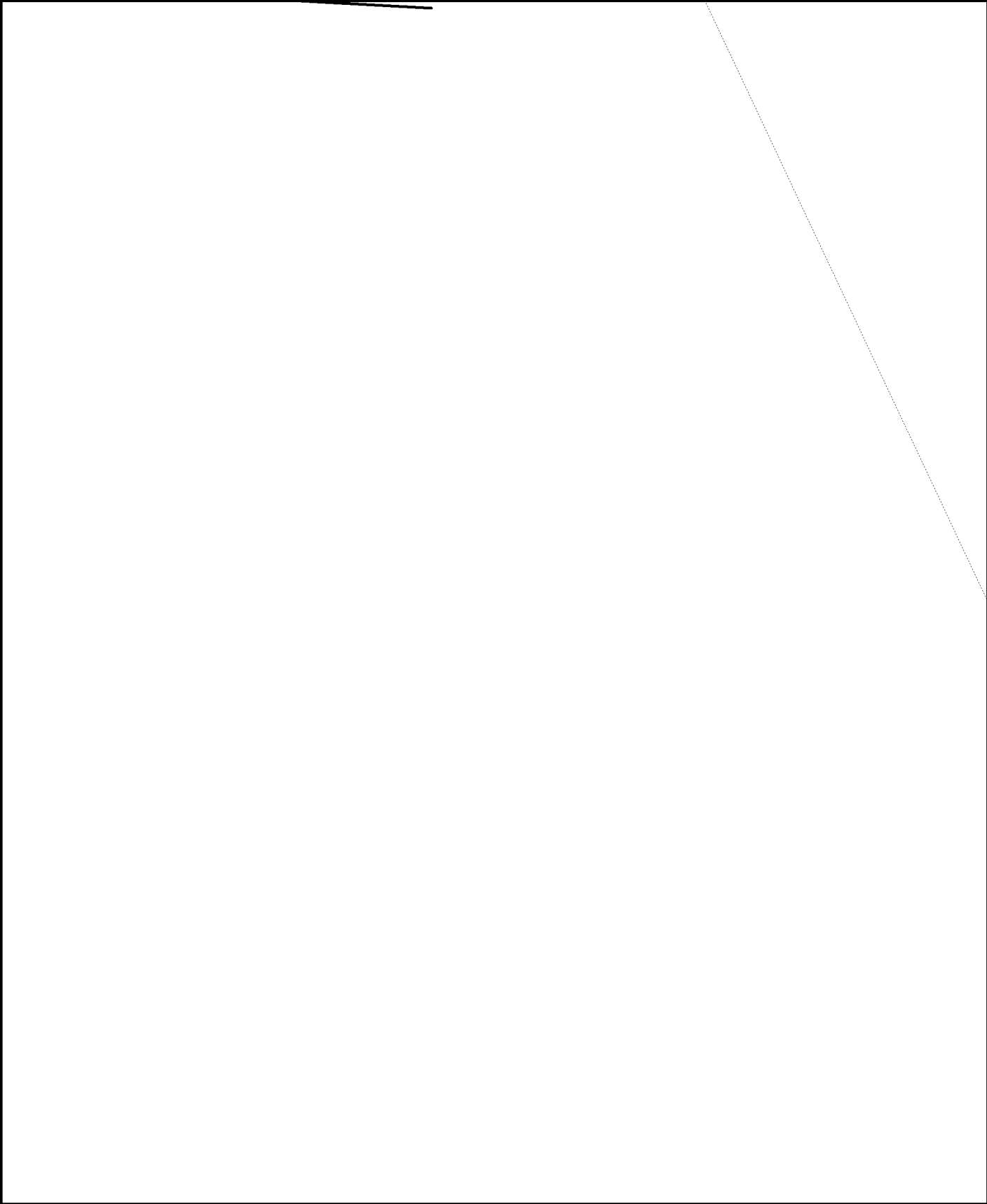
Josephine Wagoner
Doris Deming

~~TOP SECRET~~

~~TOP SECRET~~

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

~~TOP SECRET SECURITY INFORMATION~~



~~TOP SECRET~~

~~TOP SECRET~~

~~TOP SECRET SECURITY INFORMATION~~

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

~~TOP SECRET~~

~~TOP SECRET~~

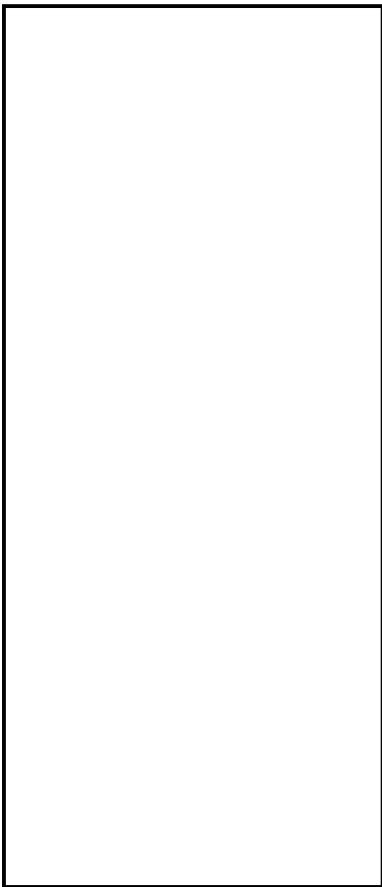
REF ID: A58738

~~TOP SECRET SECURITY INFORMATION~~

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

~~TOP SECRET~~

~~TOP SECRET~~
~~TOP SECRET SECURITY INFORMATION~~



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

~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A58738

~~TOP SECRET SECURITY INFORMATION~~

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

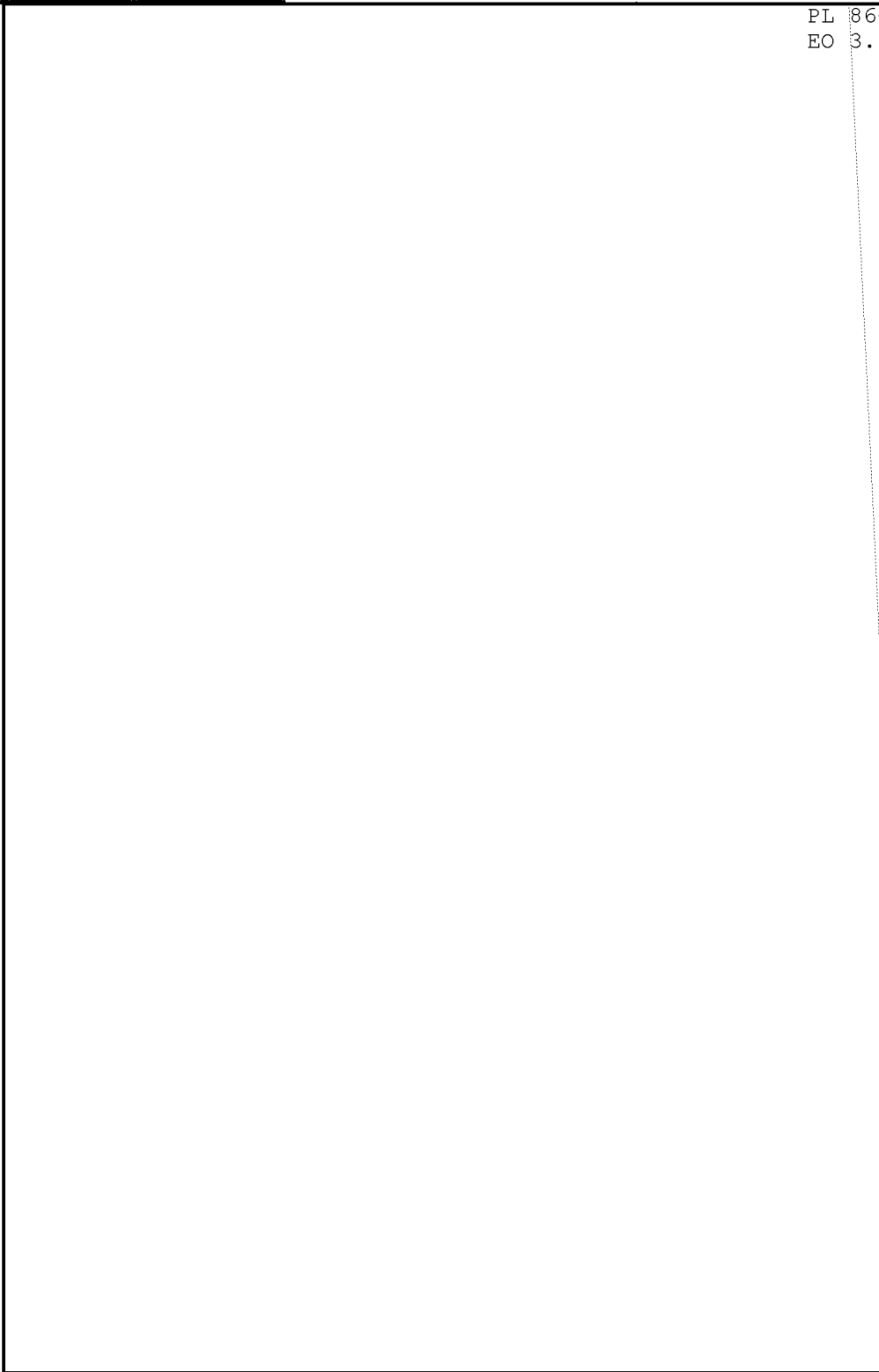


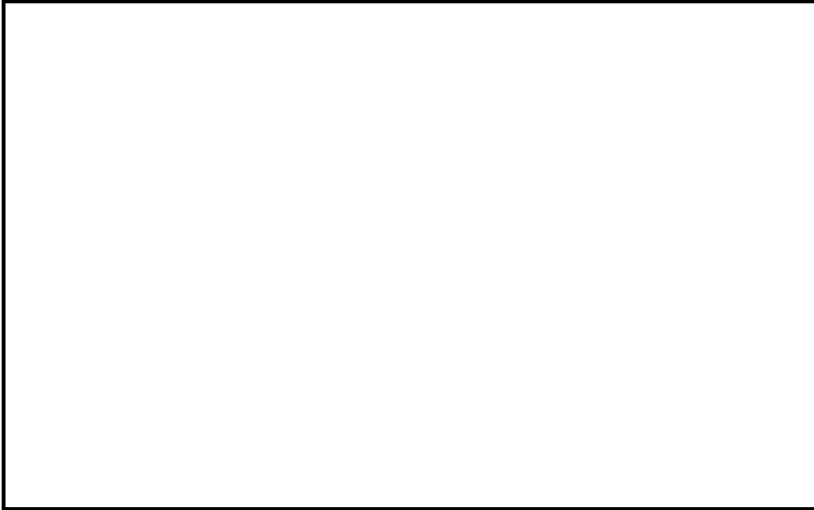
Fig 4-1

~~TOP SECRET~~

~~TOP SECRET~~

REF ID:A58738

TOP SECRET SECURITY INFORMATION



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

Fig 4-2

~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A58738

~~TOP SECRET SECURITY INFORMATION~~

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

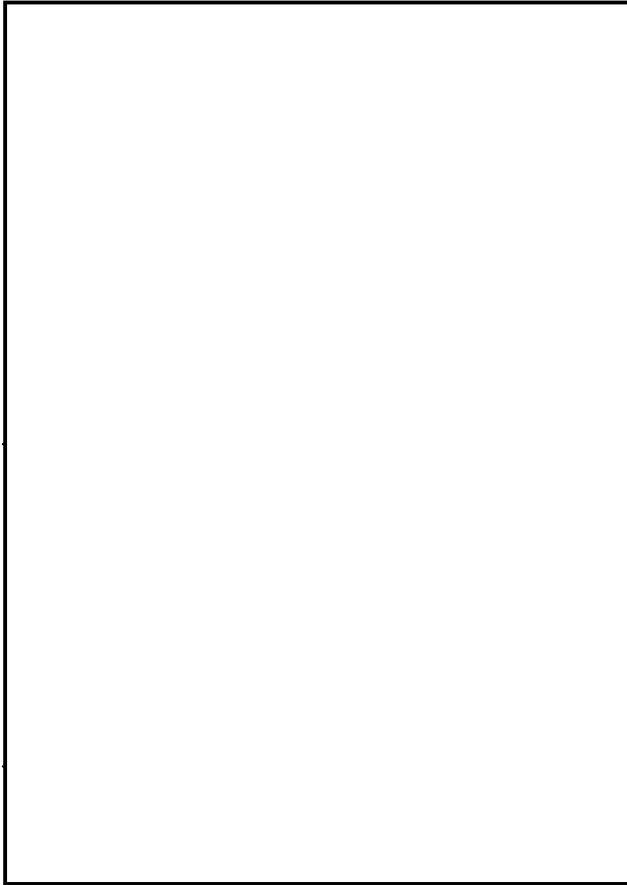


Fig 5-1

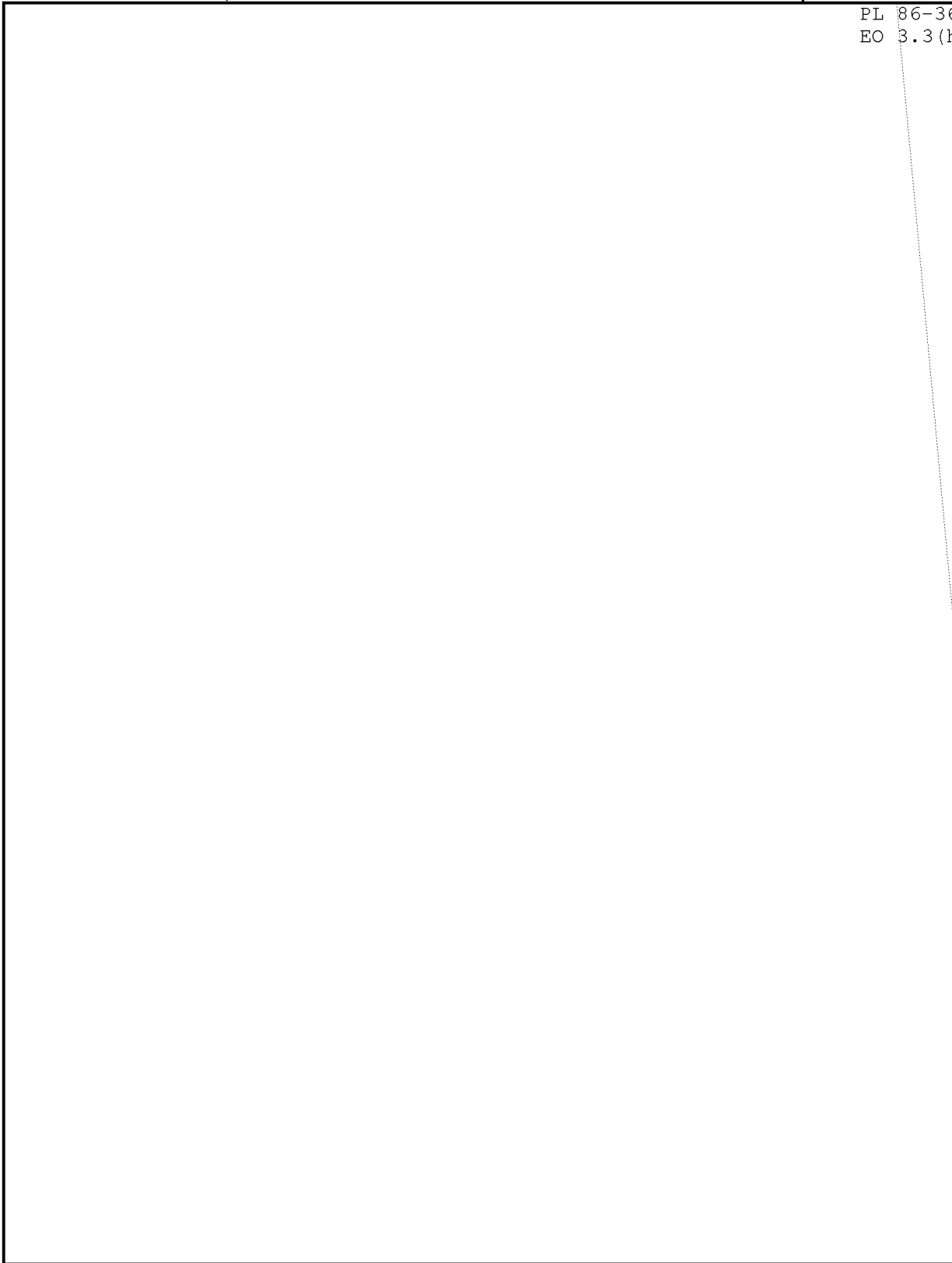
~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A58738

~~TOP SECRET SECURITY INFORMATION~~

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



~~TOP SECRET~~

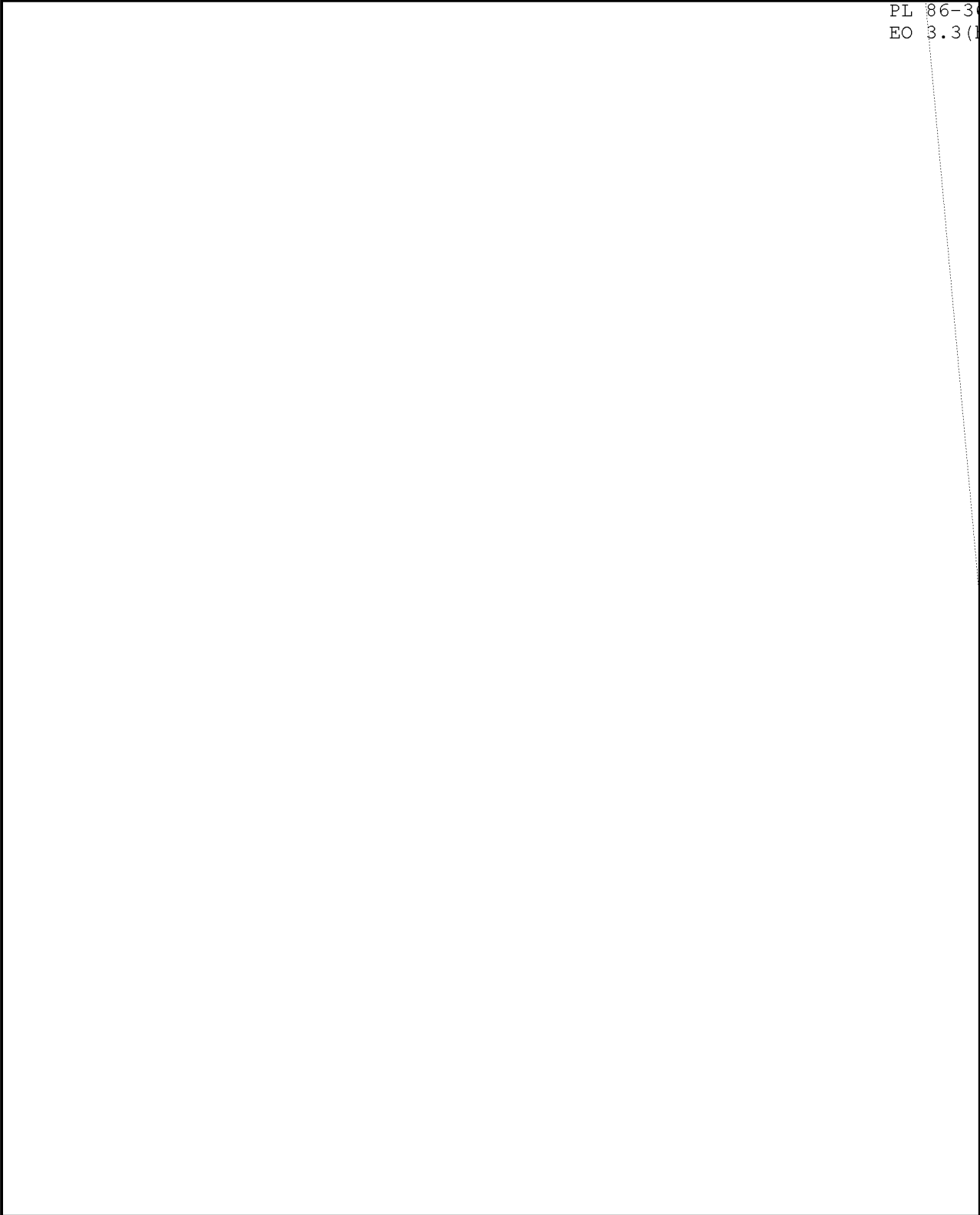
Fig 52

~~TOP SECRET~~

REF ID: A58738

~~TOP SECRET SECURITY INFORMATION~~

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



722 T V I R S H

FIG 5-2
~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A58738

~~TOP SECRET SECURITY INFORMATION~~

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

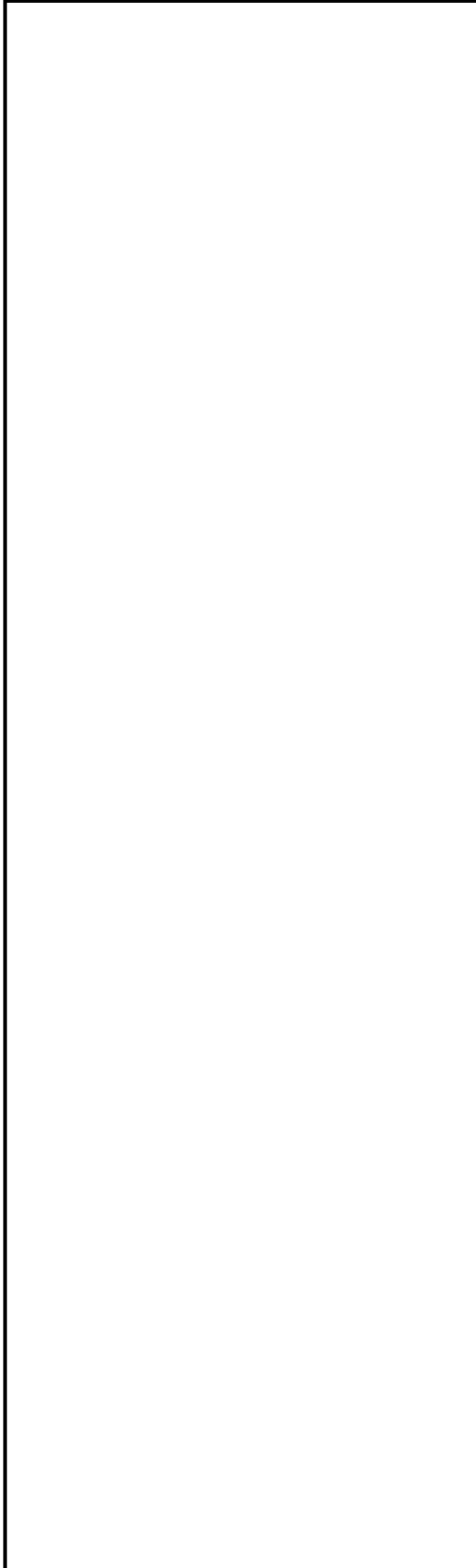


Fig 6-1

~~TOP SECRET~~

~~TOP SECRET~~

REF ID: A58738

~~TOP SECRET SECURITY INFORMATION~~



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

Fig 6-2

~~TOP SECRET~~