

~~CONFIDENTIAL~~ NACSEM NO. 7002  
DATE: September 1975

# National Security Agency

Fort George G. Meade, Maryland



National COMSEC/EM SEC Information

Memorandum

## COMSEC GUIDANCE FOR ADP SYSTEMS

~~Classified by: DIRNSA/CHCSS (NSA/CSSM 105-2)~~  
~~Exempt from GDS, EO 11652, Category 2~~  
~~Declassify Upon Notification by the Originator~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

NATIONAL SECURITY AGENCY  
Fort George G. Meade, MD 20755

COMSEC GUIDANCE  
FOR ADP SYSTEMS

LETTER OF PROMULGATION

This document is intended to provide up-to-date COMSEC guidance to cope with the security vulnerabilities created or intensified by connection or association of ADP equipment and systems with telecommunications. The information contained herein should be used by Federal Departments and Agencies in planning and taking necessary COMSEC actions to provide protection against exploitation of vulnerabilities of ADP systems.

The National Security Agency will ensure the continued timeliness and accuracy of the information contained in this document and will disseminate amendments and revisions to it.

Correspondence pertaining to this guidance document should be addressed to:

Director  
National Security Agency  
Fort George G. Meade, MD 20755  
ATTN: [redacted]

[redacted]

(b) (6)

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

Deputy Director for  
Communications Security

NATIONAL SECURITY INFORMATION  
UNAUTHORIZED DISCLOSURE SUBJECT  
TO CRIMINAL SANCTIONS

PREFACE

Development of countermeasure to computer and communications-related threats has been a major problem for ADP systems designers. In order to protect against the threats and their threat agents which are caused as a result of external communications, a multidisciplinary approach involving hardware/software, physical, personal, administrative, COMSEC and emanations security will be used to formulate potential solutions. This document is presented as guidance for designers and implementors of ADP systems and automated communications systems. The COMSEC related protective measures, as they apply to ADP and automated communications systems, are reflected by asterisks in Chapters 3 and 4.

It is recognized that other measures and techniques treated herein may be governed by other directives or issuances within the Federal Departments and Agencies, and these should be consulted as appropriate.

This document should be retained at appropriate levels for general reference. Dissemination of all or part of the information it contains to appropriately cleared individuals is encouraged. Additional copies may be obtained through the USCSB Secretariat.

## CHAPTER I

INTRODUCTION (U)

A. (U) The purpose of this document is to present a perspective view on the communications-related threats in ADP systems and in automation of communications control and information-exchange, along with a treatment of countermeasures available. The intent is to provide technical guidance on COMSEC as it applies to ADP and automated communications systems.

B. (U) Chapter 2 discusses communications-related threats and identifies the types of people who may be in a position or of an inclination to exploit the vulnerabilities of ADP systems.

C. (U) Chapter 3 deals with known techniques for reducing the vulnerability of ADP systems to identified threats.

D. (U) Chapter 4 discusses common types of computer systems which involve communications and analyzes each to show a profile of postulated threats, vulnerabilities, and corresponding protective measures which might be applied.

E. (U) The matrix in Appendix A is intended to cross-reference the discussion of categories of protective measures in Chapter 3 with that of the threat types as presented in Chapter 2. Each row of the matrix is labeled with a threat which has been identified in Chapter 2, and each column is labeled with a general protective measure. A check in the body of the chart indicates that the threat and countermeasure are relevant to each other. The check does not indicate that the countermeasure will totally combat the threat.

F. (U) The matrix also cross-references the discussion of threats with that of threat agents to indicate which types of threat agents might be likely to exploit the various types of threats. Again, this is intended only as an aid to reading the paper; in some cases the agent may only be able to exploit the threat under special conditions, such as in collaboration with system users or personnel.

G. (U) Because of the changing nature of technology and its ability to provide protection of computer data, this document will be reviewed and updated as necessary.

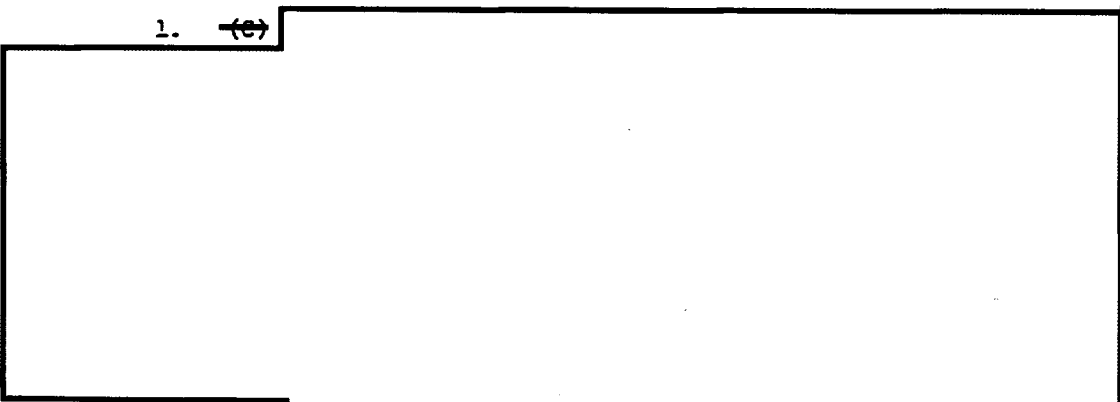
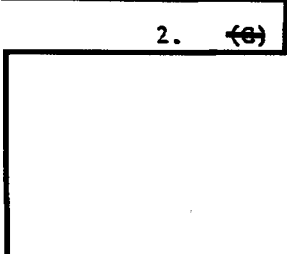
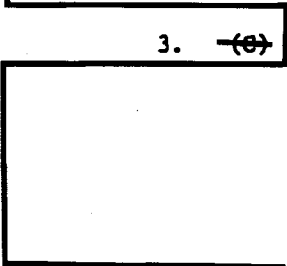
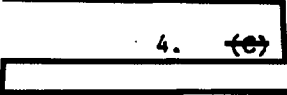
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

# ~~CONFIDENTIAL~~

## CHAPTER 2

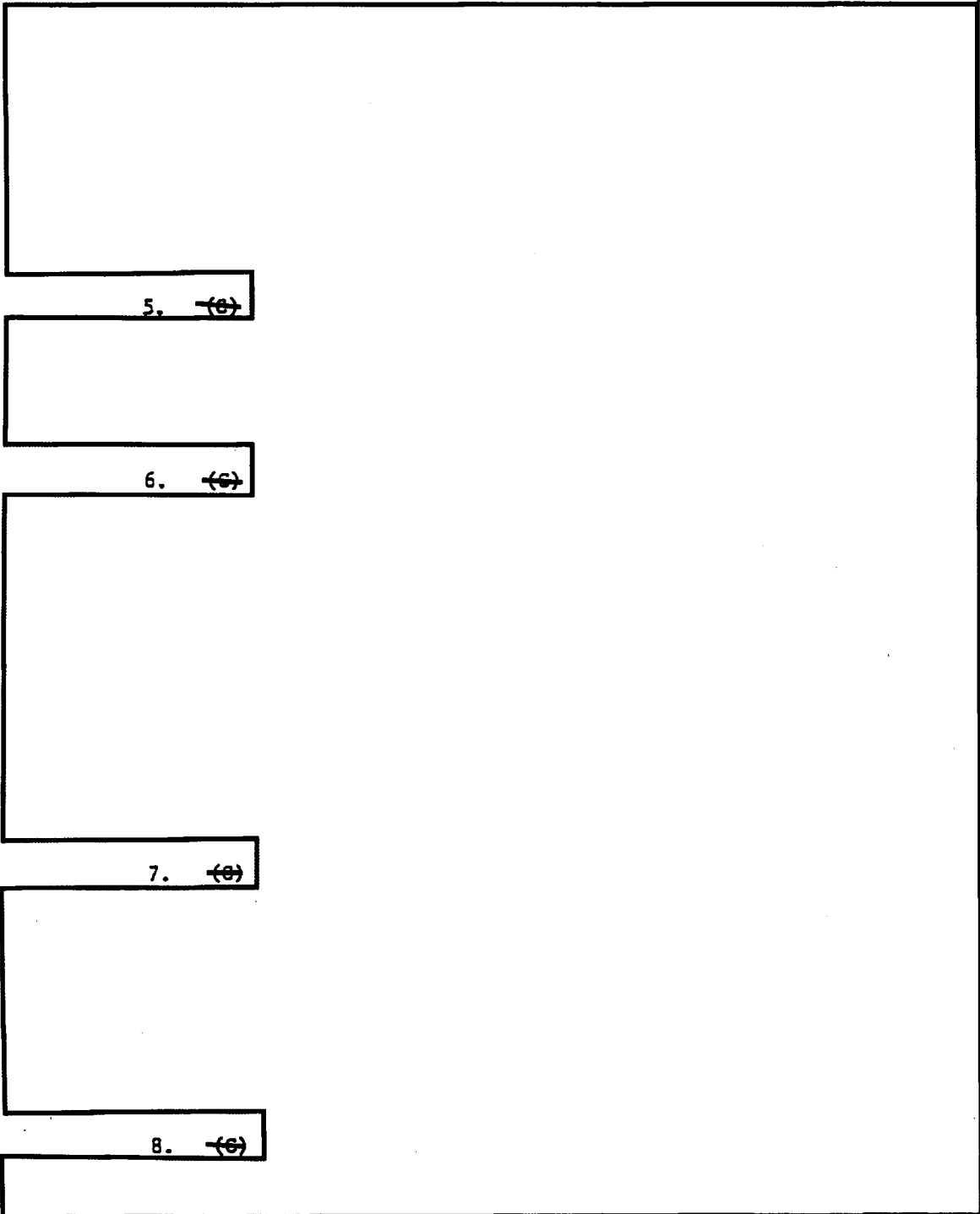
### COMMUNICATIONS-RELATED THREATS (U)

A. ~~(S)~~ TYPES OF THREATS. An ADP system may face a variety of threats resulting from or made more severe by its association with communications. It is impossible to define in advance every threat and vulnerability which will be associated with any ADP system or factors which influence the seriousness of a threat in a particular application. In addition, new systems may be subject to threats not yet encountered. However, the great majority of communications-related threats may be generally described. Each system ought to be analyzed to determine its susceptibility to each of these threats. (U)

1. ~~(S)~~ 
2. ~~(S)~~ 
3. ~~(S)~~ 
4. ~~(S)~~ 

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

~~CONFIDENTIAL~~



5. (S)

6. (S)

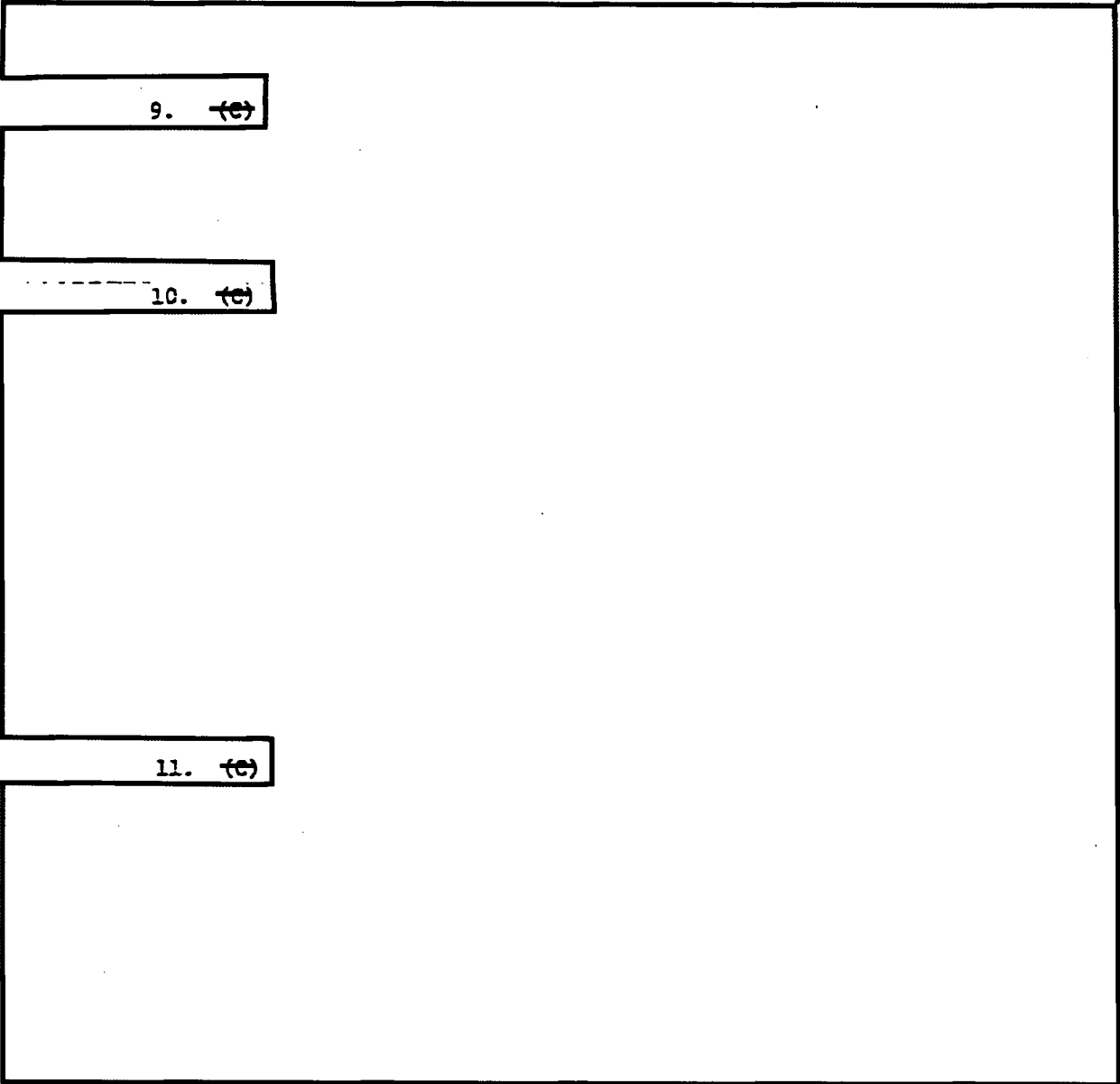
7. (S)

8. (S)

~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~



B. (U) SOURCES OF THREATS. The following are typical sources of threats to ADP systems. The classes are not necessarily separate, i.e., a foreign government or domestic antagonist may make use of cleared or uncleared system users. Anyone, regardless of his security clearance, who attacks the system must be viewed as an antagonist, whether he is outside the system, a user, an operator, or a maintenance specialist.

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

~~CONFIDENTIAL~~

1. (U) Foreign Governments. The most sophisticated antagonists with a presumed interest in exploiting or disrupting automated communications, or those associated with computers, are nonfriendly nations.

2. (c)



3. (c)



4. (U) Users with Different Clearance Levels. Where individuals are cleared to various levels of system access there is a risk of inadequate segregation of information. Thus an individual cleared for CONFIDENTIAL access may be separated from highly sensitive data only by those features of the computer/communications system which are intended to prevent malfunction and/or unauthorized probing from the distant terminal. The capabilities of such an individual for gaining unauthorized access or for maliciously probing are roughly the same as those of the uncleared user in the multilevel system.

5. (U) Authorized Personnel. An authorized person is an individual who has proven need-to-know for access to specific information or equipment. The right-to-know, which may be established by the fact of government employment or the holding of a security clearance, does not of itself constitute need-to-know. The threat from authorized personnel is similar to that cited under "Uncleared System User" and "Users with Different Clearance Levels"; it also applies to uncleared personnel who may have the apparent right, but not the need, to access unclassified information, e.g., that which is "For Official Use Only" or "Company Confidential".

6. (U) Fully-Cleared User. In some automated systems the functions are so sensitive that the ability of even trusted individuals within the system to disturb normal operation, to usurp control, or to copy information needs to be prevented or at least drastically limited. A typical system in this category would be an automated nuclear weapons system designed to permit weapons control from a distance through telecommunications; data which no one person is allowed to access would include launch codes and nuclear authenticators.

7. (U) Personnel Working with the ADP System. This group of people, which includes computer designers, programmers, operators, and maintainers, probably has the greatest opportunity to exploit or to introduce system vulnerabilities. Individuals may or may not be cleared; furthermore, because of their intimate involvement with specific portions of the system, they are better informed and in a better position to carry out threats than most other people. What might be accomplished by one of these individuals at the computer site itself can involve deliberate exploitation of hardware and/or software, as well as error. A person working within the system may be in a position to influence adversely the measures designed to protect against communications-related threats, and he also has a potential opportunity to operate undetected due to system complexity.

8. (U) Personnel Involved in ADP System Manufacturing. The computer industry has become multinational, such that often research and development, as well as the fabrication of hardware and software, are being performed in foreign countries. Changes to currently operational

hardware or software could also be originated in these places. Emitters or logical "trap doors" in computer system hardware or software therefore can be a threat.

C. (U) VULNERABILITY ASSESSMENT (U)

1. (U) The most fruitful approach to determining what countermeasures are needed against communications-related threats in an ADP system begins with a thorough examination of the system concept for threats, coupled with a weighing of the threats discovered to determine which are significant and what may be set aside as academic. With such a listing of all the threats envisioned, it is then possible to address potential countermeasures in a systematic and practical manner. In this way it may be discovered that a group of threats could be countered by a single feature. For example, accidental spillage of computer contents onto communications links may become an acceptable threat when all links are secure, all persons with access to the system are appropriately cleared and all remote terminals are protected; threats realized through deliberate probing may also be countered by these same measures.

2. (U) A highly useful technique for insuring that all threats are clearly identified is to prepare a report which includes the following:

Description of the system configuration, with major features, user capabilities, expected clearance conditions, and similar features defined.

Identification of applicable threat sources, with ordering as necessary, and an evaluation of the protection needed.

Documentation of factors that influence system sensitivity. This would cover the nature of the information to be protected, including its perishability, and the impact of such threats as interception, intrusion, system disruption, and unauthorized actions on the part of the system users, operators, and maintenance personnel. These factors should be assigned weights/values in order to assist the authority responsible for protecting information in performing a comparative evaluation.

Identification, in the light of the previous factors, of threats which must be countered within a specific degree of probability and of those which it is desirable, but not essential, to counter.

3. (U) The vulnerability assessment should, of course, be followed up with an overall test and evaluation after the application of protection. Such evaluation would include detailed analysis of the

system to determine the effectiveness of the various protective measures. Such analysis may also be supplemented by appropriate testing of developmental and/or operational models of the system.

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

# ~~CONFIDENTIAL~~

## CHAPTER 3

### PROTECTIVE MEASURES (U)

A. (U) GENERAL. Once a vulnerability assessment has identified the ADP system threats which should be countered, appropriate protective measures can be chosen and incorporated into the system. For most ADP systems, they may be found under the categories listed in this chapter. The choice of specific techniques within these categories depends upon the characteristics of the system involved, how it is used, the type and sensitivity of the information requiring protection, the severity of the threats, the costs and technical feasibility of constraints involved, the acceptable range of risk of loss or compromise, as well as who the potential threat agents are. It must be stressed, however, that these countermeasures are not necessarily available or sufficient to guarantee security; sometimes no amount of protection can combat all system threats. Countermeasure selection should, therefore, include steps to ascertain their effectiveness in the type of situation at hand.

### B. ~~(S)~~ CRYPTOGRAPHIC PROTECTION (U)

\* 1. ~~(S)~~

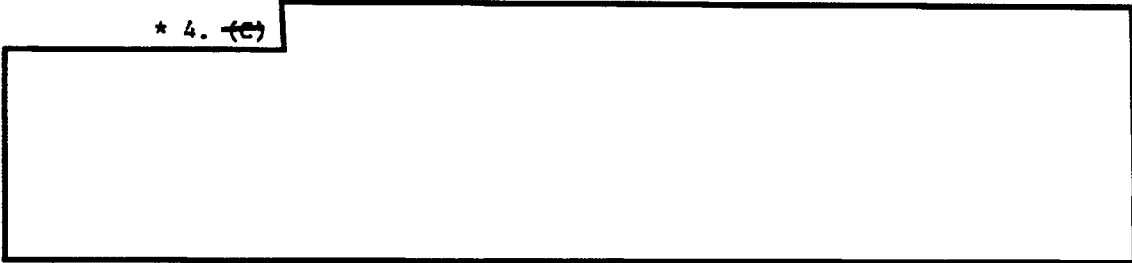
\* 2. ~~(S)~~

\* 3. ~~(S)~~

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

~~CONFIDENTIAL~~

\* 4. (c)

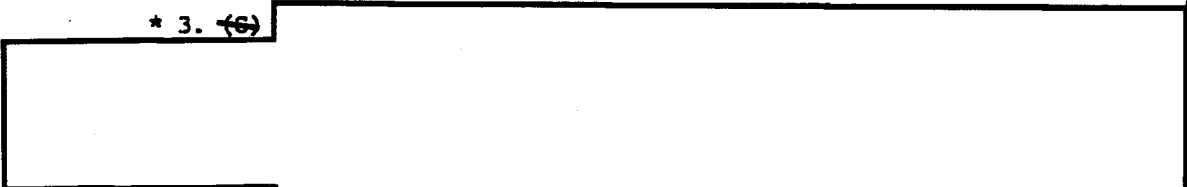


C. (c) AUTHENTICATION (U)

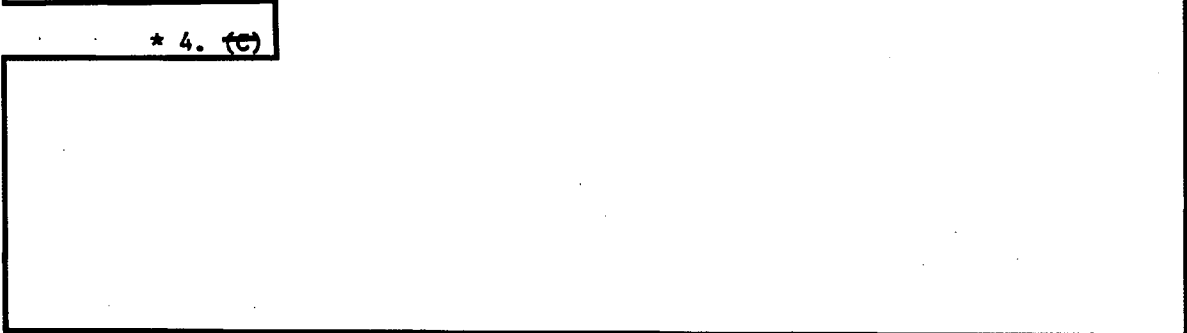
\* 1. (U) The term authentication as used herein includes the capability to do, as appropriate, any of the following by either cryptographic or other means: identify and verify the user (either human or hardware) to the ADP system and vice versa; detect accidental or deliberate changes in data during its transmission; and detect or prevent insertion or replay of transmissions. Encryption of messages or physical protection of communications equipment and media may be critical for ensuring the effectiveness of these authentication techniques.

\* 2. (U) Authentication is in most cases essential when one or more terminals are shared and not all users of a terminal are authorized access to the same level of information. Authentication may also be useful, particularly if supplemented with special hardware features at the central computer, in identifying the capabilities of users entering a multilevel or a resource-sharing computer system through uncleared terminals. Current techniques include passwords (e.g., randomized sequences of characters known only to their holders and to the computer system), physical keys, plastic cards containing magnetic strips, and identifiable unique human features such as fingerprints.

\* 3. (c)



\* 4. (c)



~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

\* D. (S)

E. (U) CLOSED SYSTEM OR BENIGN ENVIRONMENT. An obvious way to eliminate the uncleared or partially cleared system user as a threat agent is to operate the system with all personnel and facilities cleared to and protect for the highest level of any information handled within it, while encrypting any physically unprotected communications media. This approach does not prevent attacks from the outside, but it does reduce the required security measures to primarily those in the need-to-know and physical and personnel security areas.

F. (U) PHYSICAL SECURITY MEASURES (U)

\* 1. (U) Cryptographic Equipment and Material. If the cryptography within or associated with ADP systems is to serve its purpose, the cryptographic variables must of course be denied to potential attackers and therefore must be physically protected. This applies, for example, to variables employed with an encryption process and to authenticator lists. In addition, cryptographic algorithms themselves may require protection.

2. (U) ADP Equipment and Material. Appropriate physical security controls employed to safeguard the equipment apply not only to the computer equipment itself and at its terminals, but also to such removable items as printouts, magnetic tapes, magnetic disc packs, punched cards, etc. The point is to protect not only the user's data and programs, but also security measures in the system. If parts of the computer system (e.g., magnetic discs, tape files, or copies of machine listings) contain unusually sensitive data or need to be physically isolated during maintenance procedures, it may be necessary to separate them physically and to control access to them independently. This applies

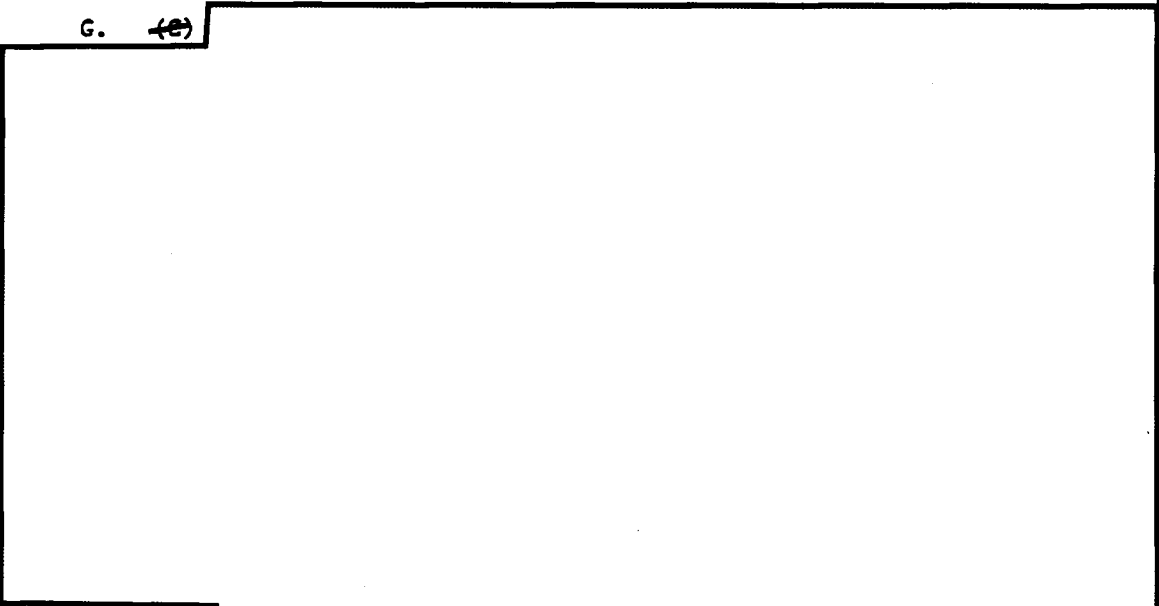
~~CONFIDENTIAL~~

# ~~CONFIDENTIAL~~

to the environmental facilities required to provide reliable operation of the system.

\* 3. (U) Protected Wireline Distribution System (PWDS). . A PWDS is a communications system, or that portion of a communication system, to which electromagnetic and physical safeguards have been applied to permit secure electrical transmission of unencrypted information over a wireline. Furthermore, a PWDS is designed so that compromising emanations are not exploitable from outside the physically controlled area. For example, remote terminals throughout a large building may be connected to a central computer located within the building by means of a PWDS provided all persons within the building are assumed to be non-hostile. A PWDS can be an alternative to cryptography for protecting communicated information when relatively short distances and controlled areas are involved.

G. ~~(S)~~



H. ~~(S)~~



I. (U) CONFIGURATION CONTROL. Because computer systems are so complex in both hardware and software it is necessary that they be designed to permit reasonable and continual verification that they in fact function as intended. Modular design concepts provide a means of isolating to a large extent the security features, thus minimizing the number of interactions between them and other operations. Thorough analysis and testing of any system changes before their implementation is advisable to protect against undesirable effects on the ADP system's security features or posture. After the system is operational, configuration control of both hardware and system software serves to verify that undetected changes have not taken place.



## CHAPTER 4

THREATS AND COUNTERMEASURES APPLIED TO SYSTEMS (U)

(U) This treatment is intended to relate the previous discussions of threats and countermeasures to various functional types of computers. The purposes are to give more meaning to the threats and countermeasures previously outlined; to show how the threats and countermeasures vary with system function; to indicate how some communications related threats can be defeated through protective measures internal to the computer; to show gross capability of current protective technology; and to define further the gaps in current protective technology.

(U) To these ends the more common functions will be arbitrarily broken into the classes defined below. The classes are not complete and all-inclusive, but rather representative. The intent is to simplify treatment by dealing with the role of a computer unit, or collocated complex of computers, in carrying out a basic type of function. It is accepted that in reality the situation is not so simplistic in that such a collection of computers, or even a single computer, may serve a number of separate functions defined below. In this instance, some combination of countermeasures based upon the system's operational environment and threat analysis would be appropriate. It is also accepted that computers at two or more locations may be tied together for interworking and that the composite of functions served in such a case becomes even more complex. Computer networks would fall within this category.

(U) A chart form of presentation is used as a means of relating specific threats, countermeasures, and limitations to current technology for the various functional classes of computers. Here the threats and countermeasures are amplifications of those previously outlined, and their intended meaning is as described. Again, the listings, while intended to be as nearly comprehensive as possible, cannot cover all situations or all details for any one system. A variety of operational and environmental factors influence the risk of loss or compromise of classified information and, thus, the appropriate countermeasures.

A. ~~(S)~~ COMMUNICATIONS PROCESSORS (U)

1. (U) Brief Description. Computers as communications processors are used to support and facilitate the communication of information rather than to execute user programs. As such, they generally perform automated message processing such as formatting, packetizing, and routing. Some basic types of communications processors are described below:

Switching System. In the role of switching, the purpose of the computer is to receive incoming messages and to relay them to intended recipients, usually according to formatted header information. The computer is not concerned with the actual texts of messages; it simply performs routine message handling tasks.

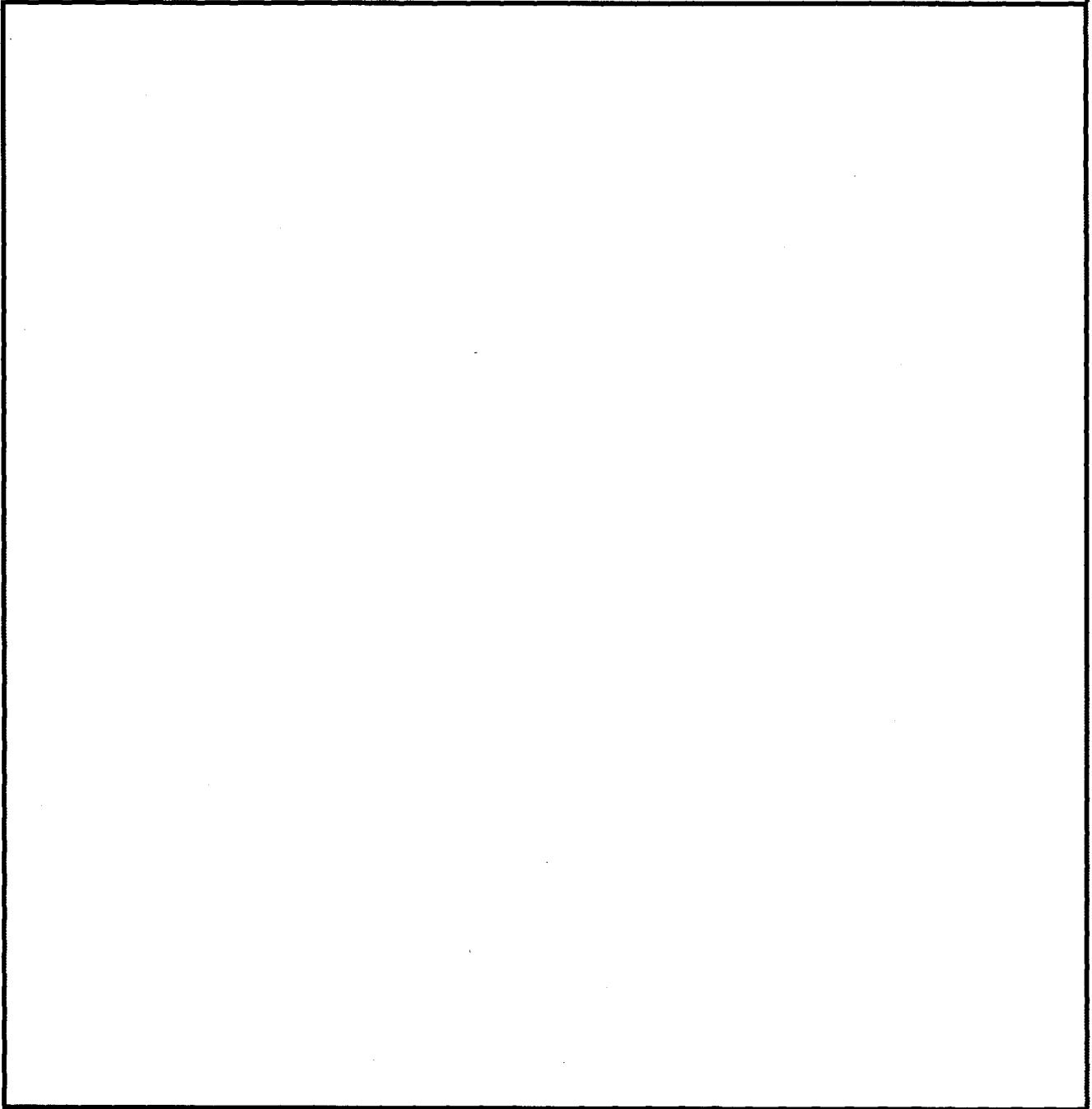
Internal Distribution System. A special case of a switching system is the local message distribution system. This type of system is in most ways similar to a full-fledged communications switch, but it may carry special functions to serve a local set of subscribers.

Front End Processor. A programmable front end processor is similar to an automated switch as described above. More particularly it is a computer (often a minicomputer) which serves another computer or device, acting as an interface between it and the communications circuit(s) to which it is connected. Typical tasks performed by the front end processor on incoming/outgoing data are line or data concentrating, preprocessing, message formatting and/or switching, and code converting.

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

~~CONFIDENTIAL~~

2. ~~(S)~~ Typical Threats and Countermeasures - Communications Processors. (U)

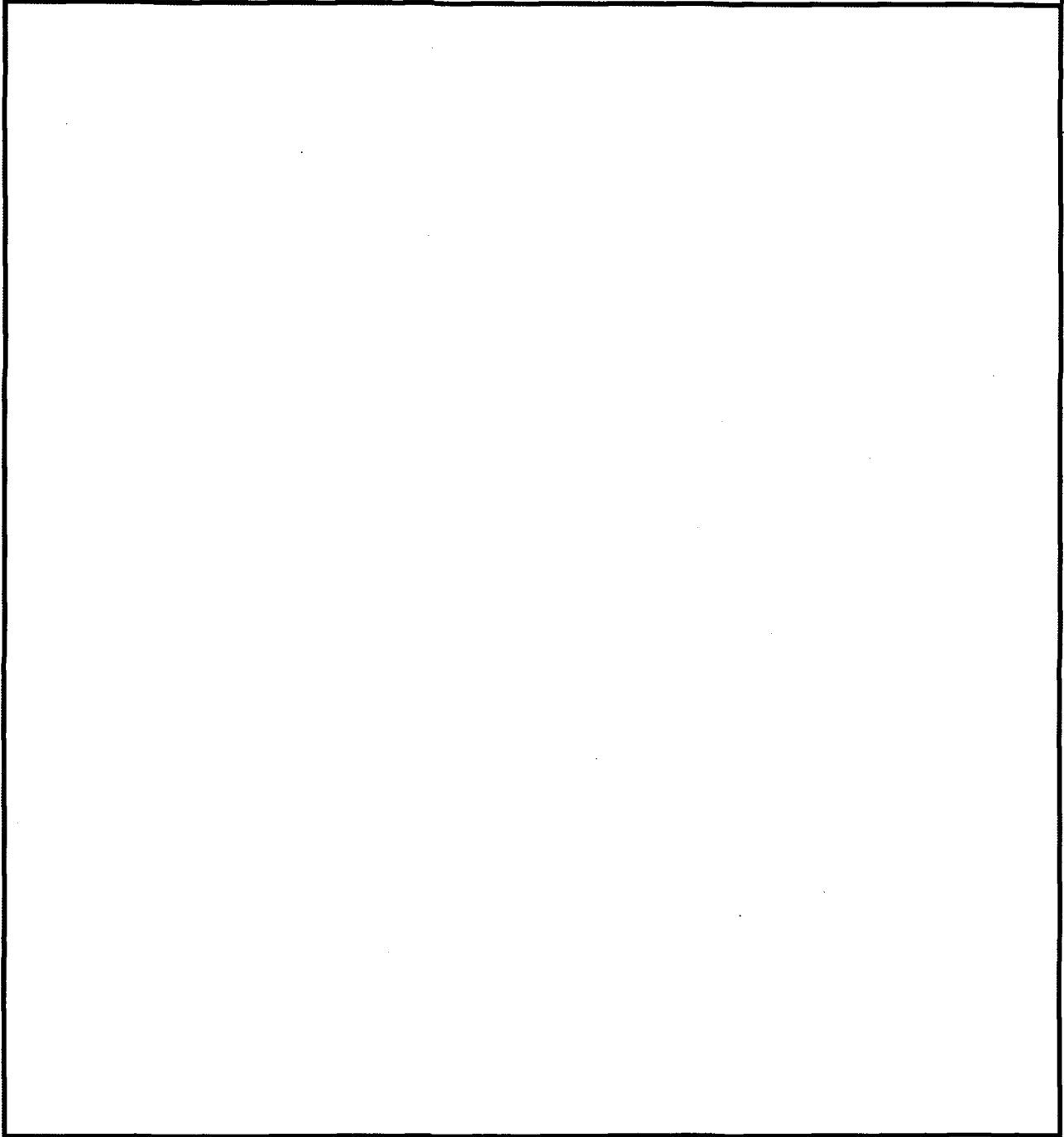


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Processors. (U) Typical Threats and Countermeasures - Communications

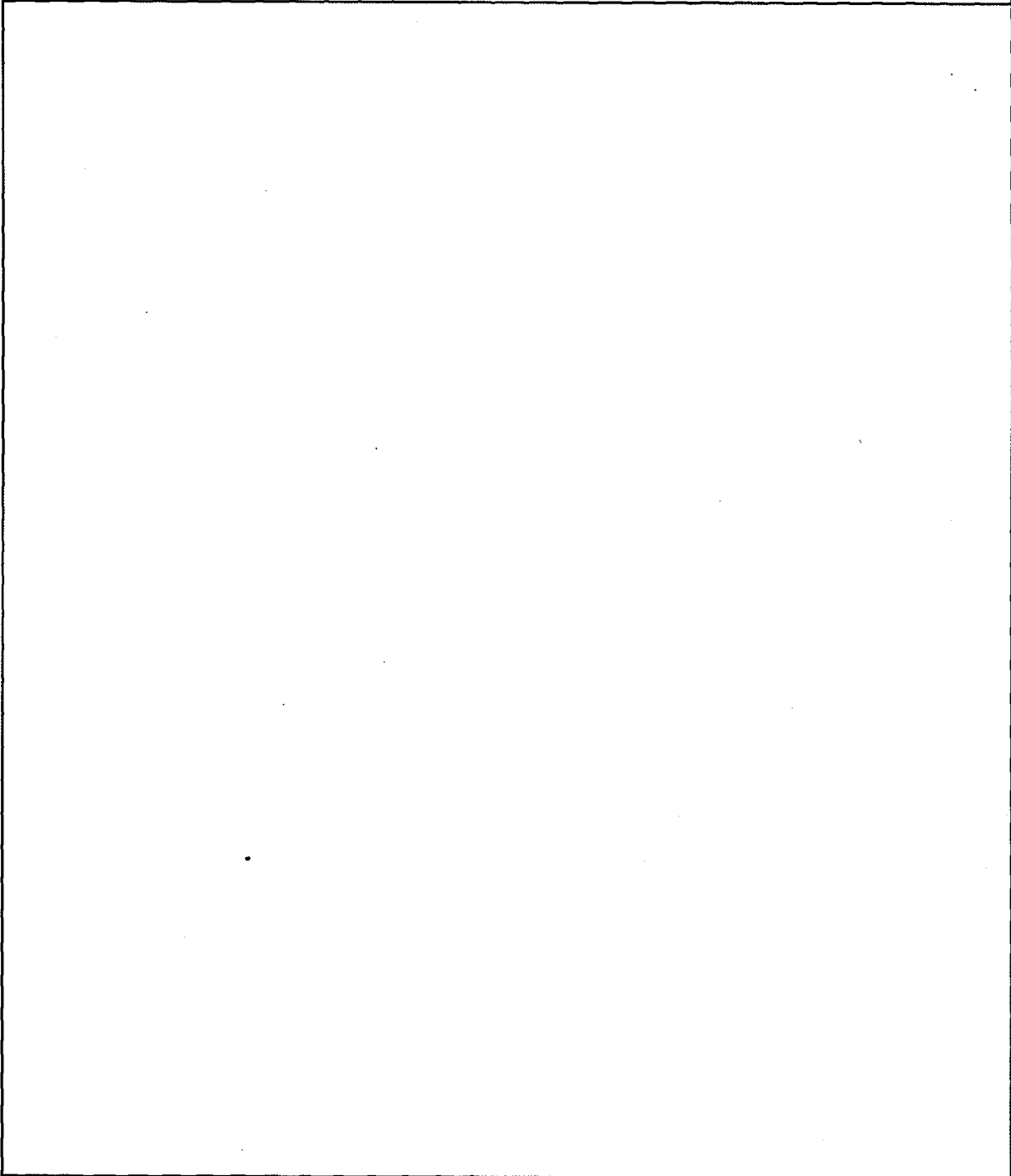


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Communications  
Processors. (U)



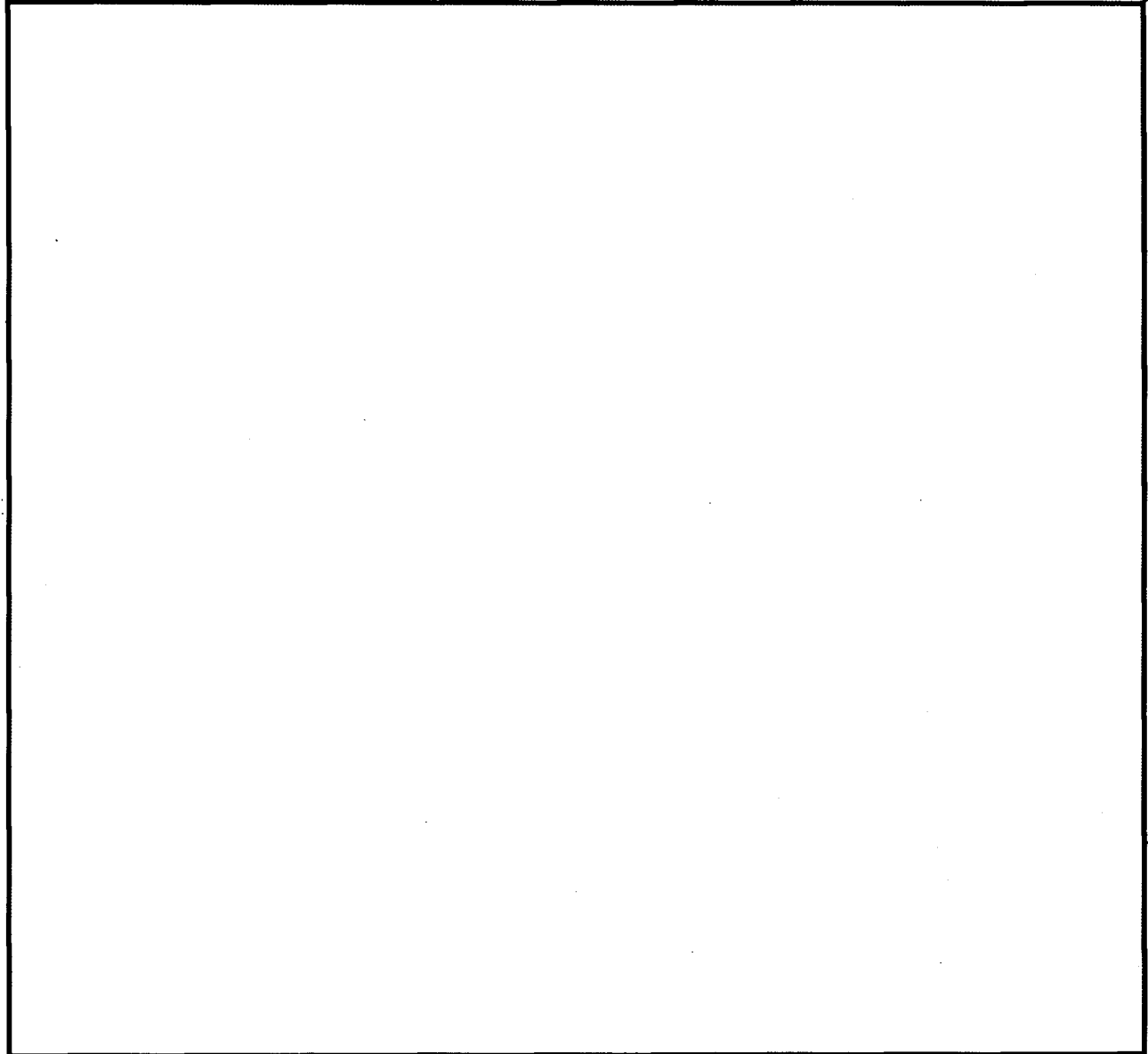
<sup>18</sup>  
~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Communications

Processors. (U)

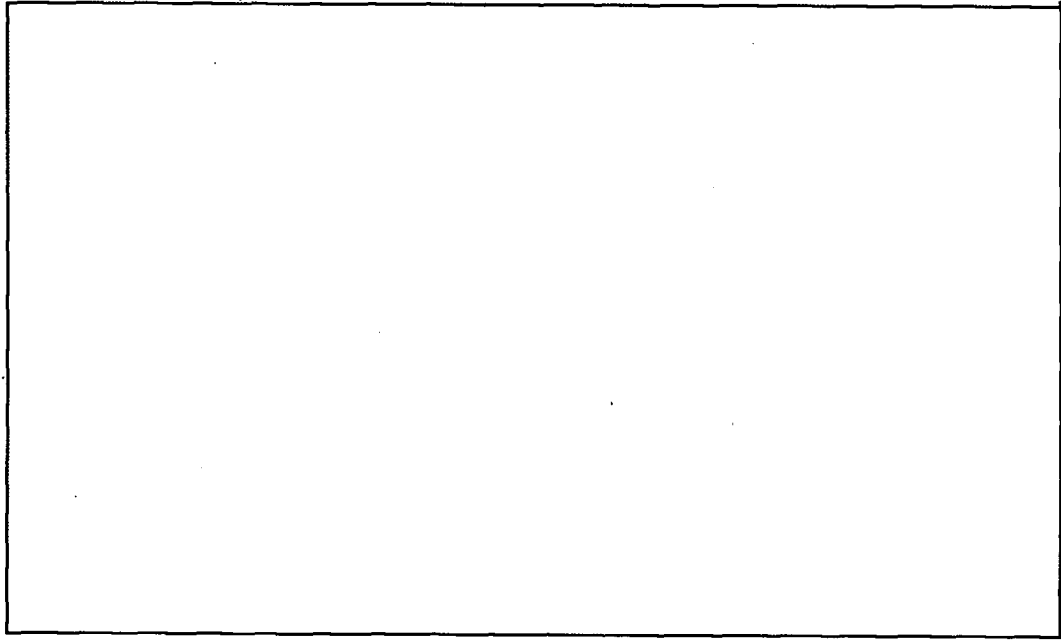


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Processors. (U) Typical Threats and Countermeasures - Communications



~~CONFIDENTIAL~~

~~CONFIDENTIAL~~\* 3. ~~(S)~~B. ~~(S)~~ INFORMATION STORAGE AND RETRIEVAL (ISR) SYSTEMS (U)1. Brief Description (U)

(U) Information storage and retrieval systems of interest have three principal hardware components:

The user terminal at which the user inserts his requests for or changes to stored information and which displays all or part of the reply;

The CPU which performs the system control functions such as query processing, data base searching, information retrieving, and response routing;

Bulk storage devices for storing data elements.

(U) Typically the data base is very large, while the desired response consists of a relatively small portion dealing with a specific subject. Structured indexing and searching schemes may be employed in the system to allow the user to formulate his request in predefined terms and to speed the processing of the query. The system may include: multiplexed communications between the CPU and terminals; the limiting of individual file access to specified groups or individuals; using the CPU, possibly from the terminals, to provide services in addition to storage and retrieval (e.g., data file manipulation or remote use of controlled and validated program modules).

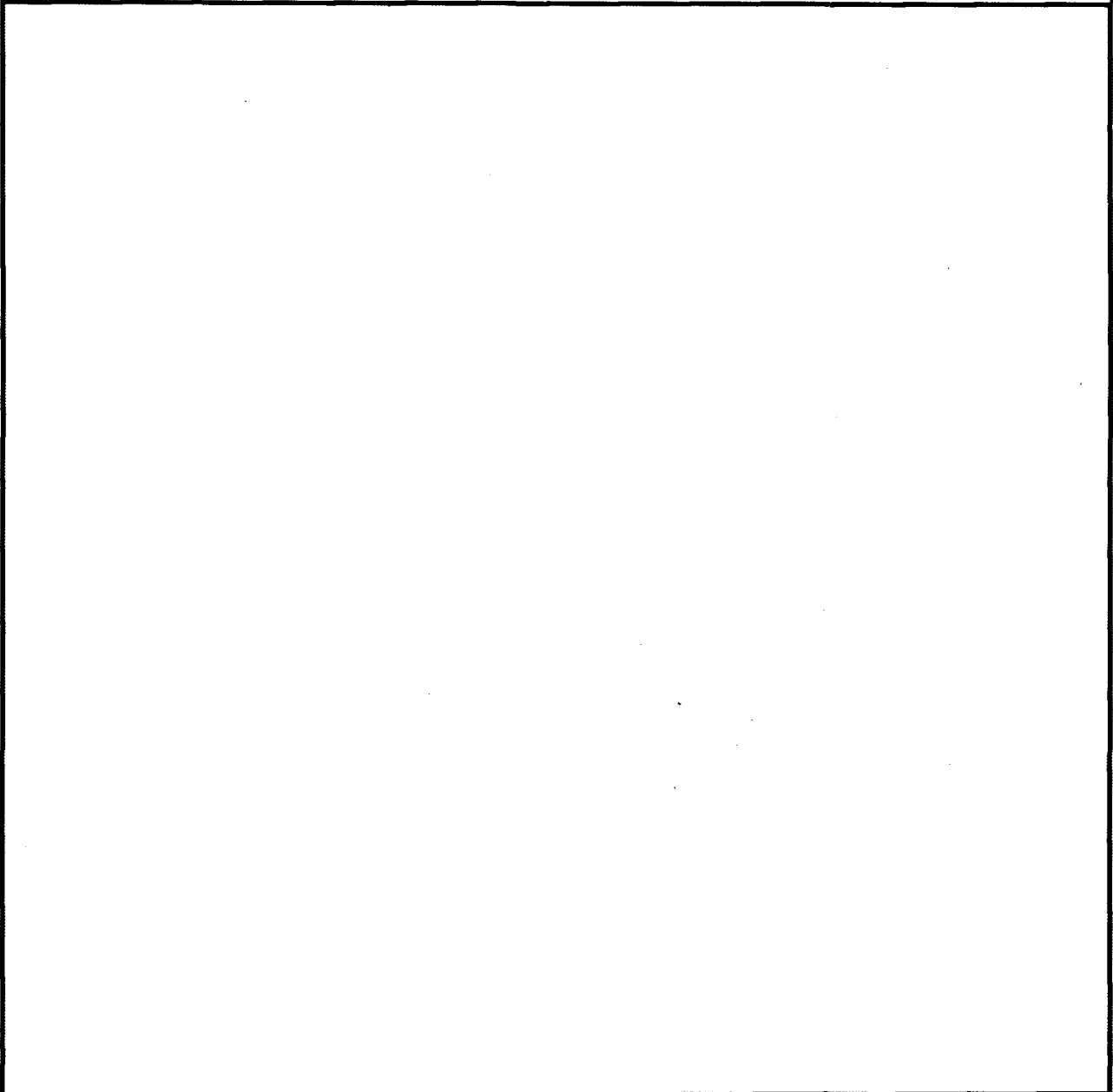
~~CONFIDENTIAL~~



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

~~CONFIDENTIAL~~

2. ~~(S)~~ Typical Threats and Countermeasures - Information Storage and Retrieval Systems (U)

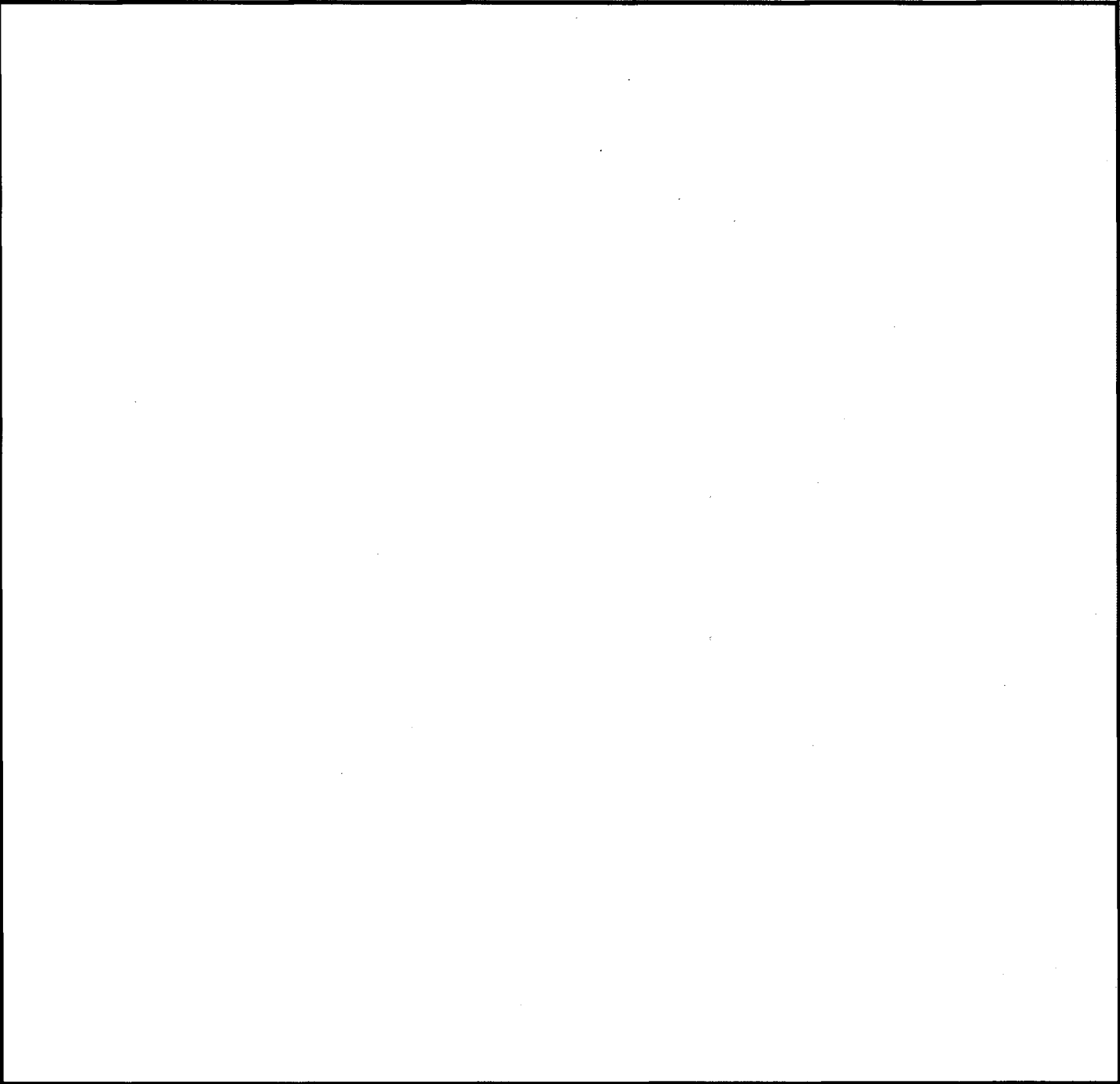


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Information Storage  
and Retrieval Systems (U)

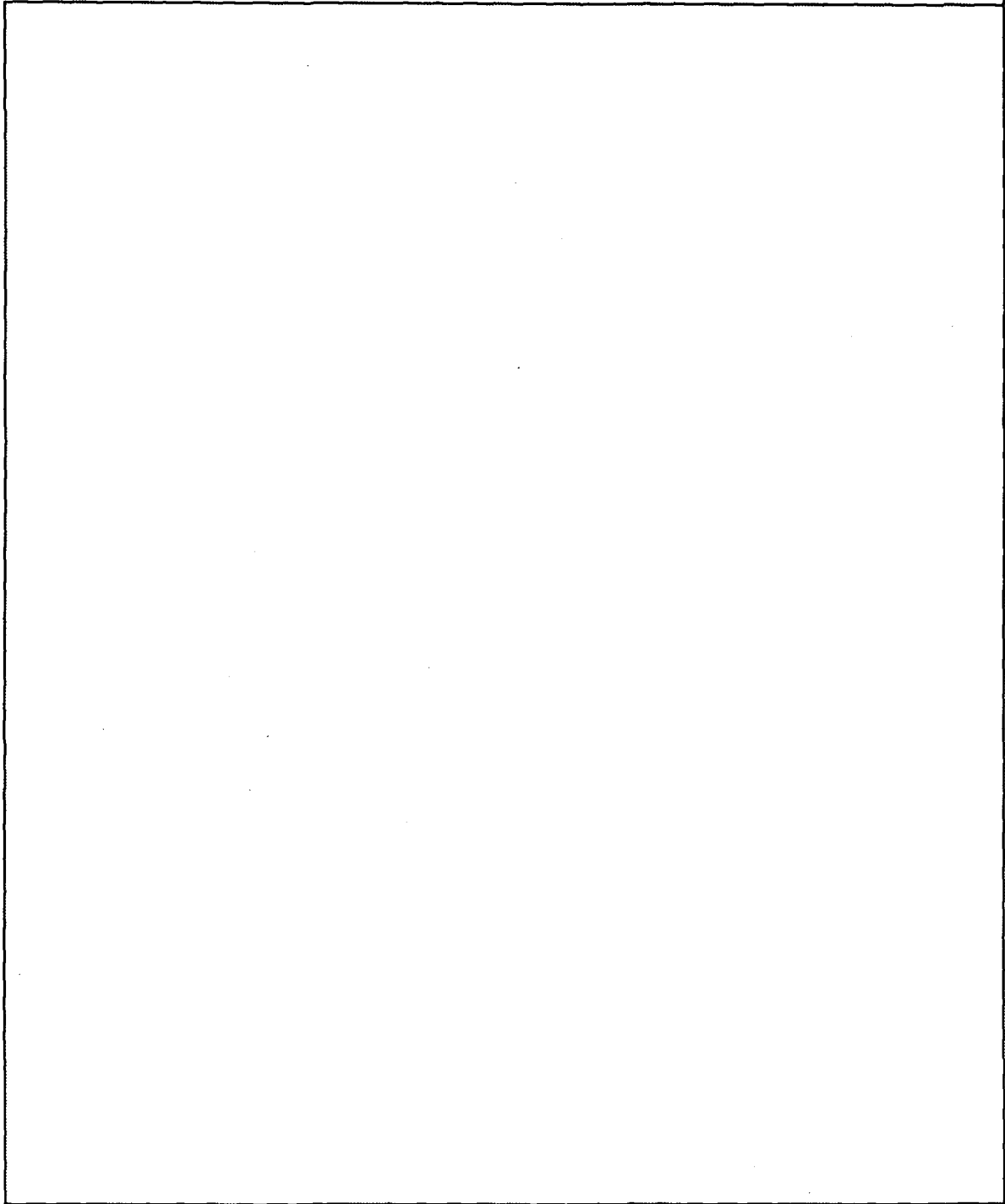


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Information Storage  
and Retrieval Systems (U)

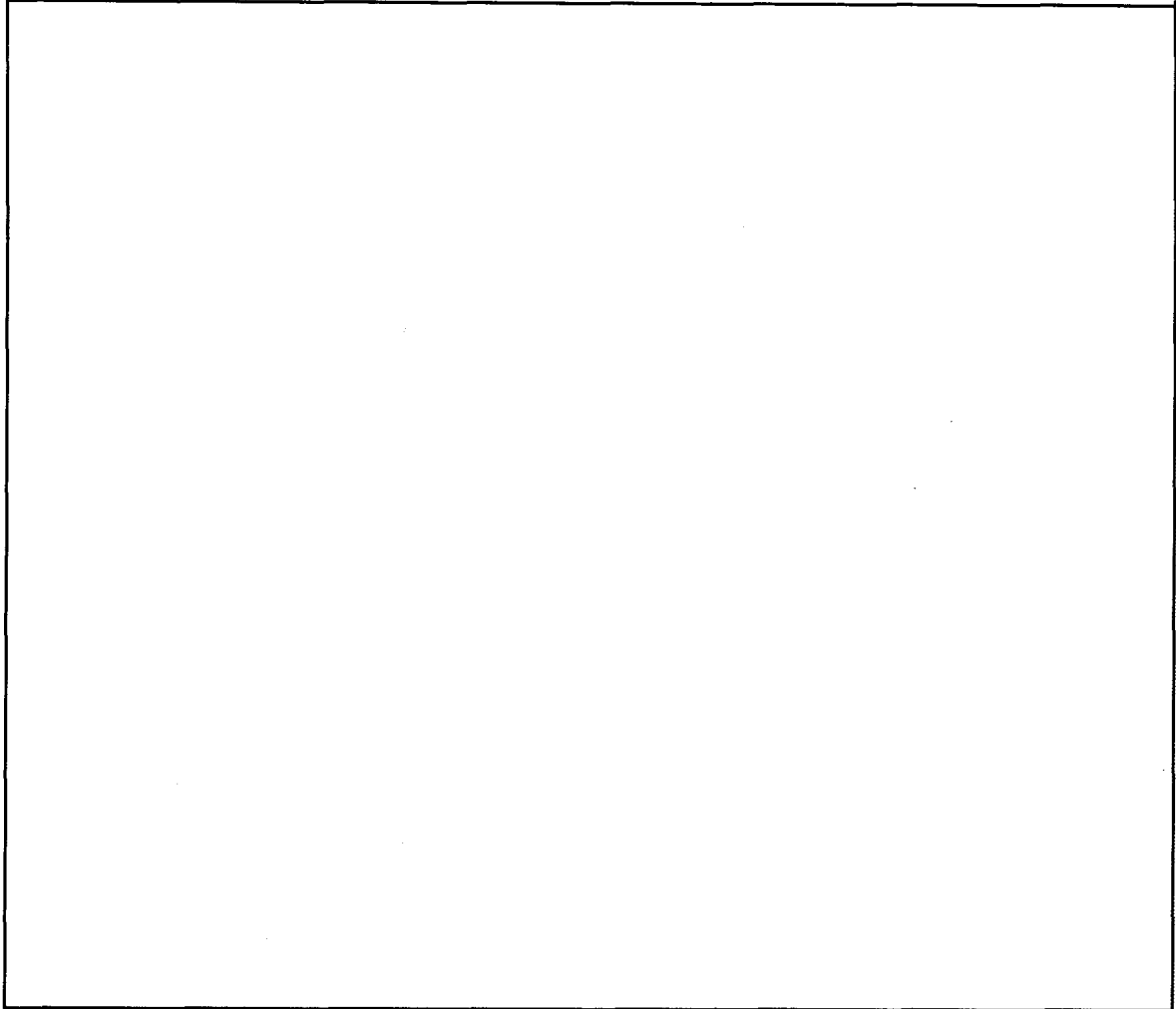


~~CONFIDENTIAL~~

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

# CONFIDENTIAL

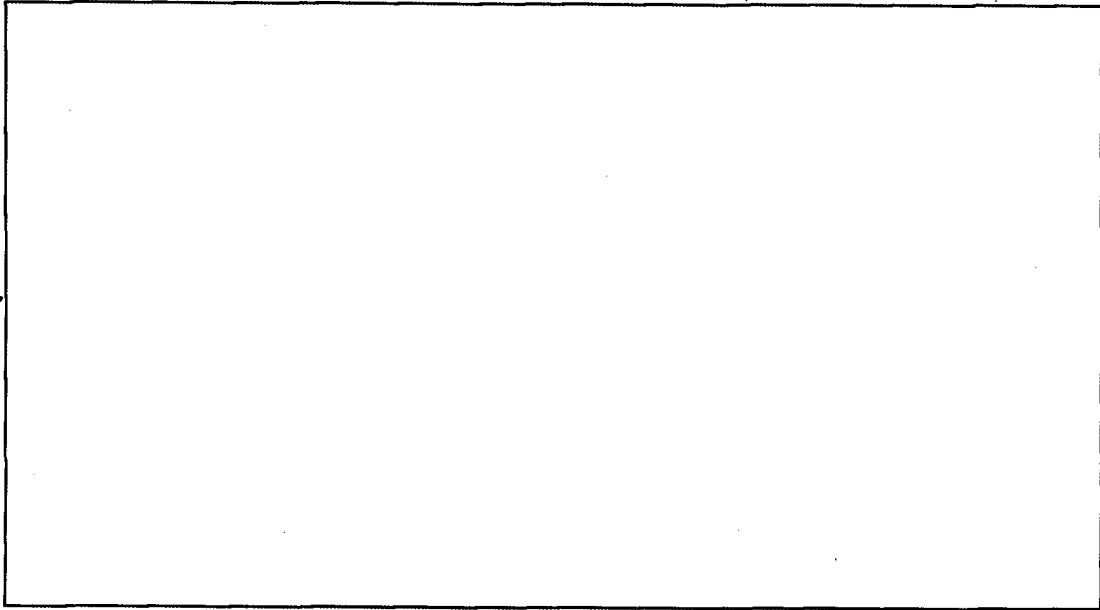
Typical Threats and Countermeasures - Information Storage  
and Retrieval Systems (U)



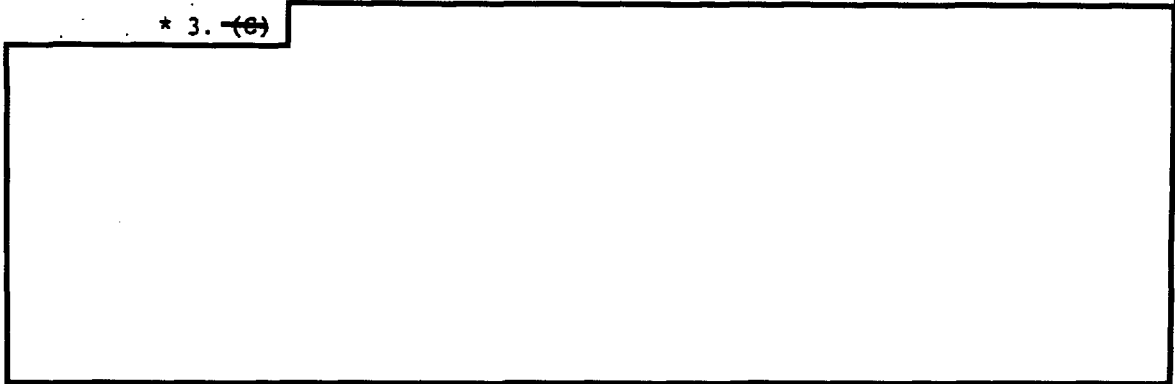
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Information Storage and Retrieval Systems (U)



\* 3. ~~(S)~~



C. ~~(S)~~ USER PROGRAMMABLE SYSTEMS (U)

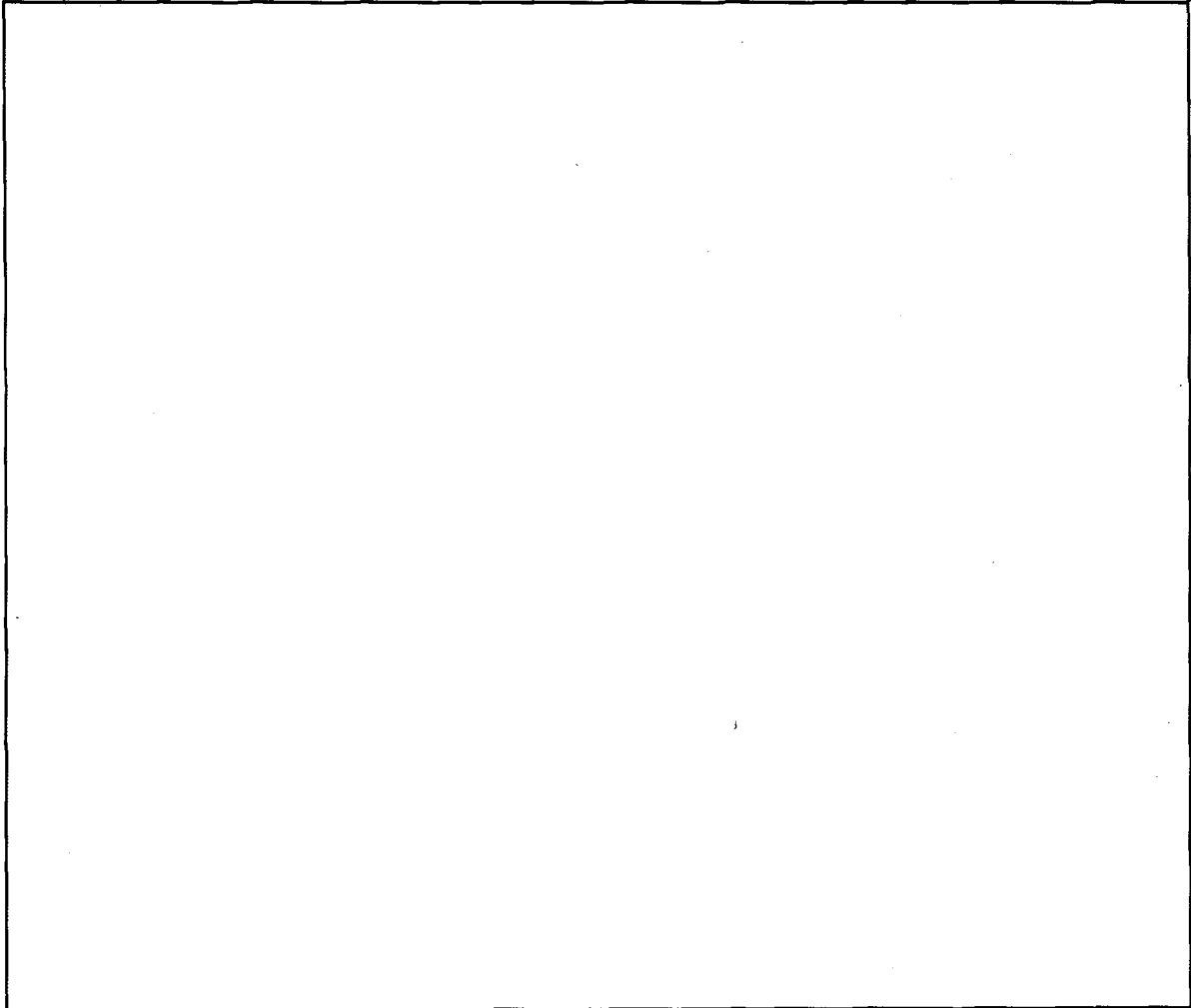
1. (U) Brief Description. The term user programmable system designates an ADP system on which the user is afforded some measure of programming capability by which he can exercise the manipulative capabilities of the computer. The remote user has at his disposal one or more higher level languages and might also have a machine or assembly language capability.

~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Systems 2. ~~(S)~~ Typical Threats and Countermeasures - User Programmable  
(U)



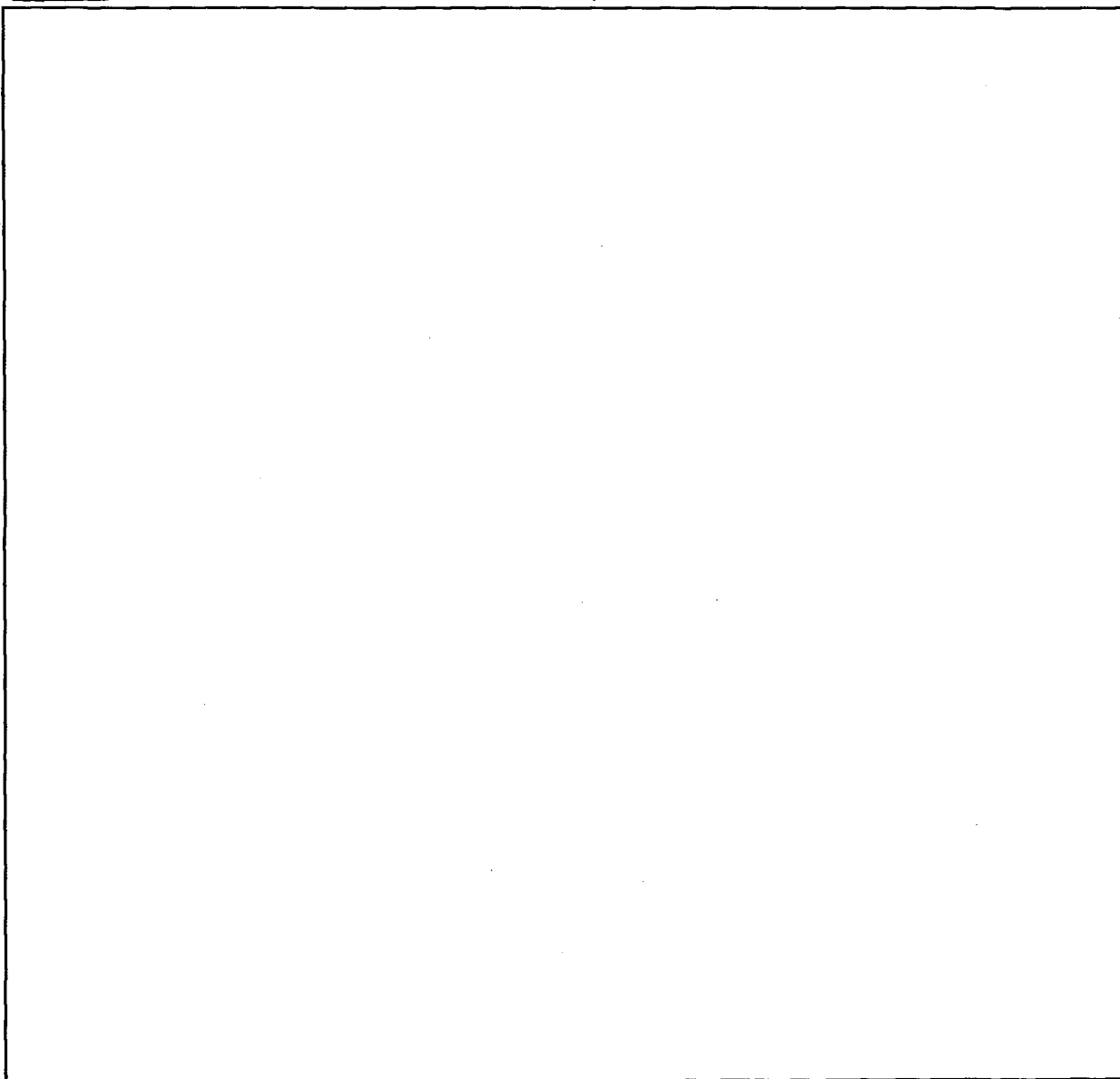
~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - User Programmable

Systems (U)



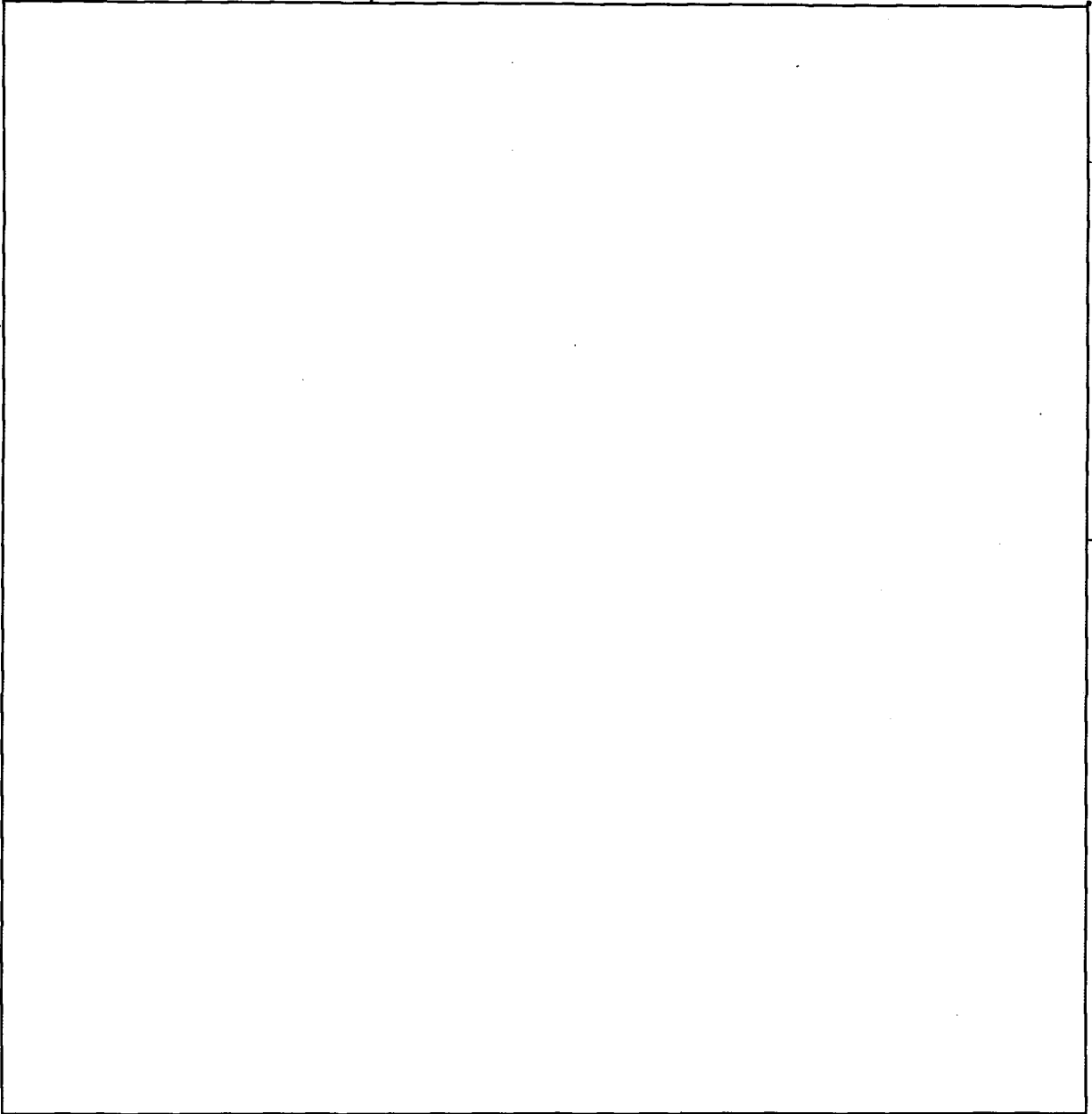
~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - User Programmable

Systems (U)



~~CONFIDENTIAL~~

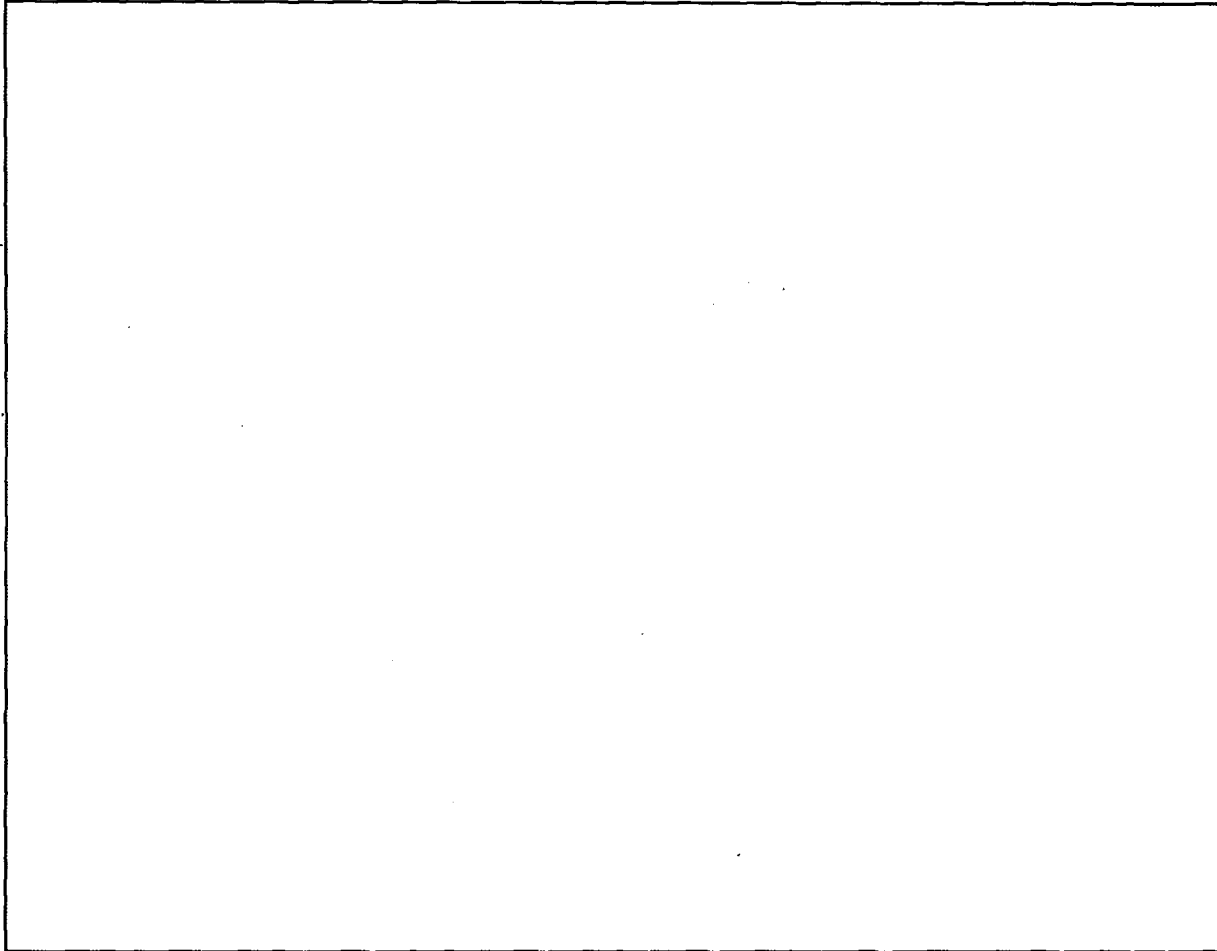


(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - User Programmable

Systems (U)



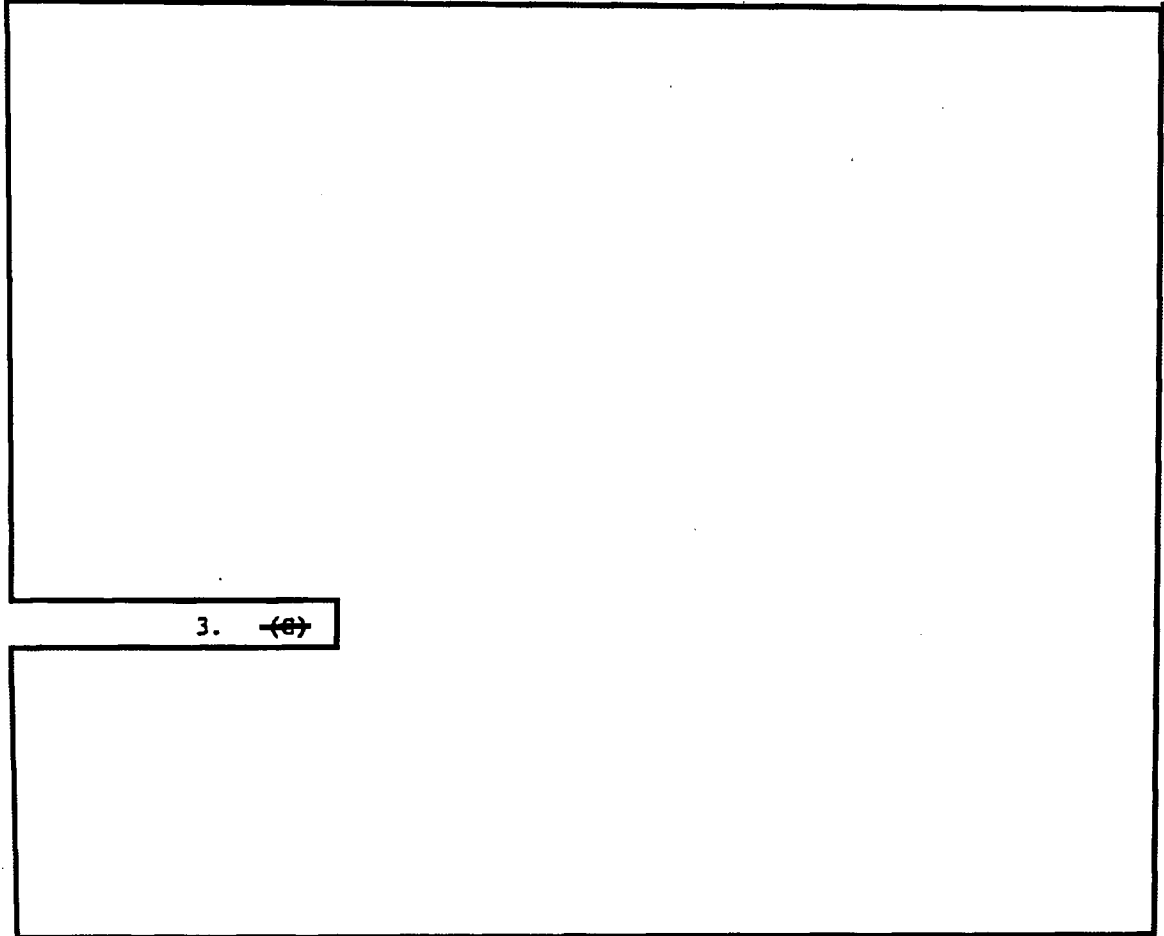
~~CONFIDENTIAL~~

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

# ~~CONFIDENTIAL~~

## Typical Threats and Countermeasures - User Programmable

Systems (U)



3. ~~(S)~~

### D. ~~(S)~~ DEDICATED PROCESS CONTROLLERS (DPC) (U)

1. (U) Brief Description. DPC's are preprogrammed processors designed to perform a limited repertoire of specific functions related to remote activities. For example the computer directs (controls) the guidance of a missile, the arming of a weapon, the attitude of a satellite, or the operation of remotely controlled sensors through telecommunications. This type of computer has its program loaded before the system becomes operational; no provision is made for remote programming of any kind. In general program loading is conducted under stringent control procedures to verify that it has been performed correctly.

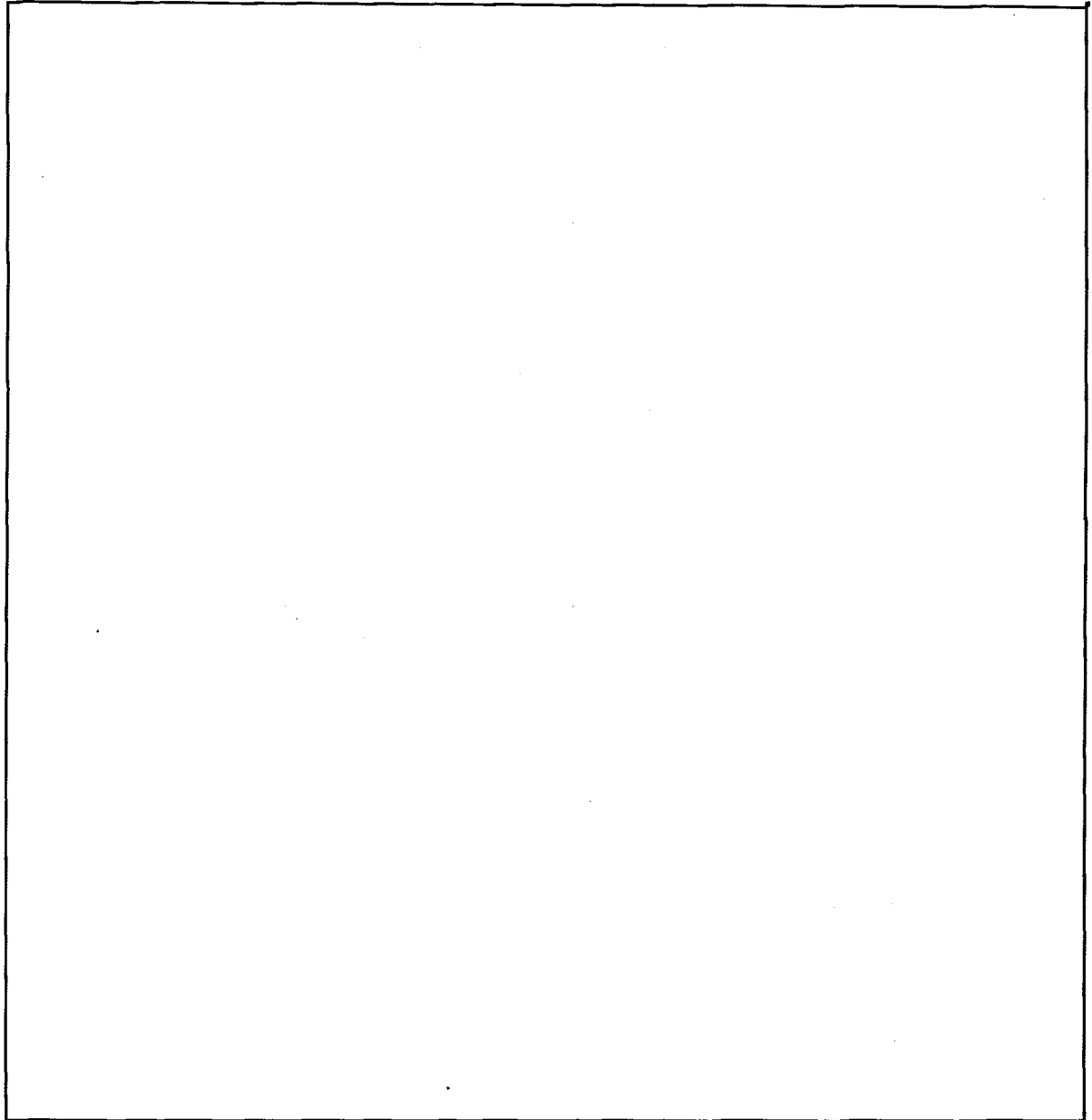
Commands and data normally are rigidly formatted and are entered into the system either automatically or by an operator. The commands are used to activate and deactivate control programs. In certain cases secure commands are used to protect the entry and operation of DPC systems; in other cases commands perform a status reporting or telemetry gathering function. Data may also be input and massaged by prestored programs in an intelligence gathering environment.

The limited capabilities and the restrictive modes of operation of DPC systems preclude many of the threats found in most computer systems. The design of these systems is based upon limited access (commands) to the remote computer. Some of these systems are automatic and others are semiautomatic; the degree of automation is a function of the actions required by an operator to effect a command, i.e., he may push a button, type on a keyboard, or insert punched cards. The recipient of the commands generally consists of an unmanned equipment that must first decode and then act upon the command.

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

~~CONFIDENTIAL~~

2. (C) Typical Threats and Countermeasures - Dedicated Process  
Controllers (U)



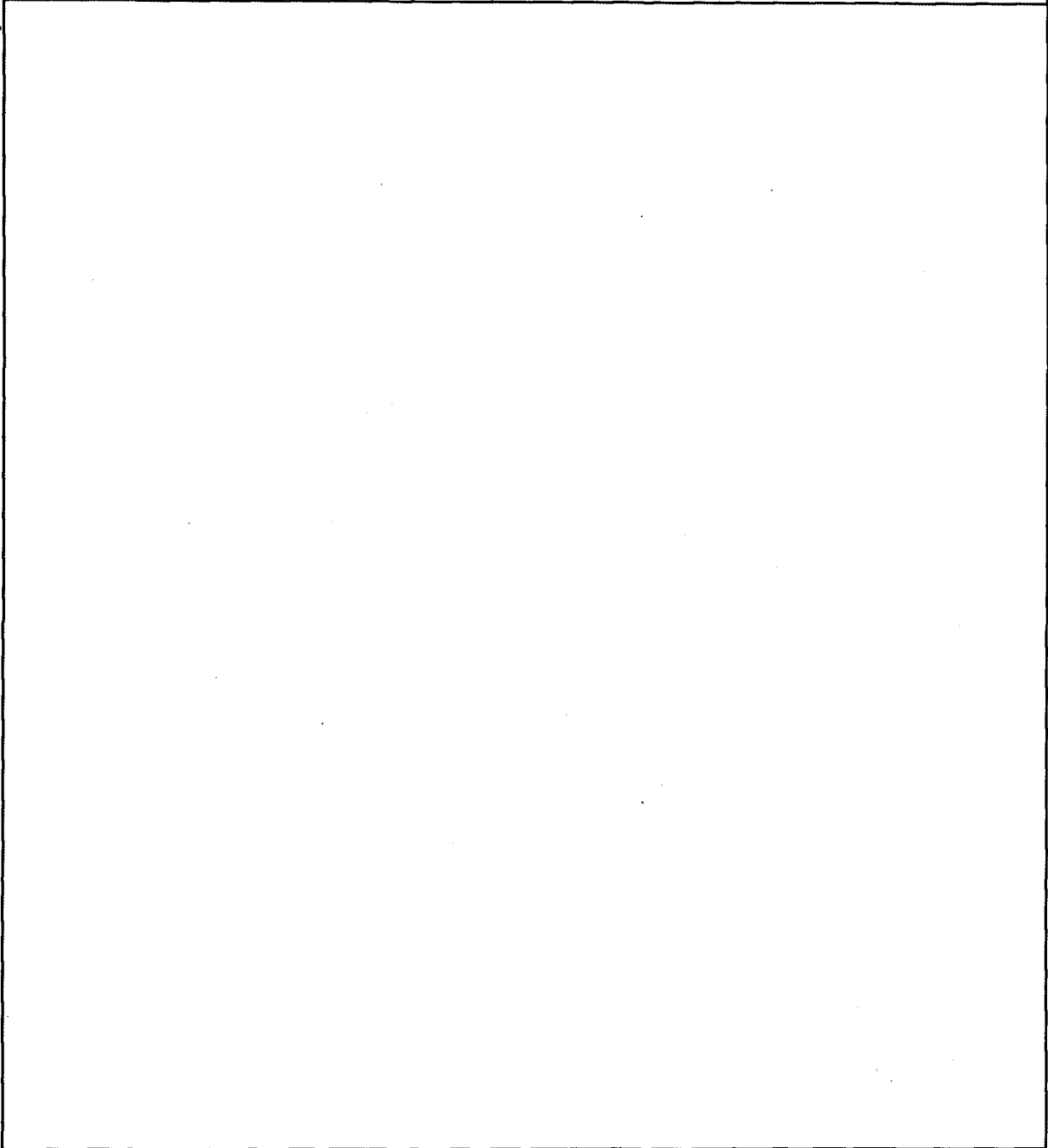
~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Dedicated Process

Controllers (U)

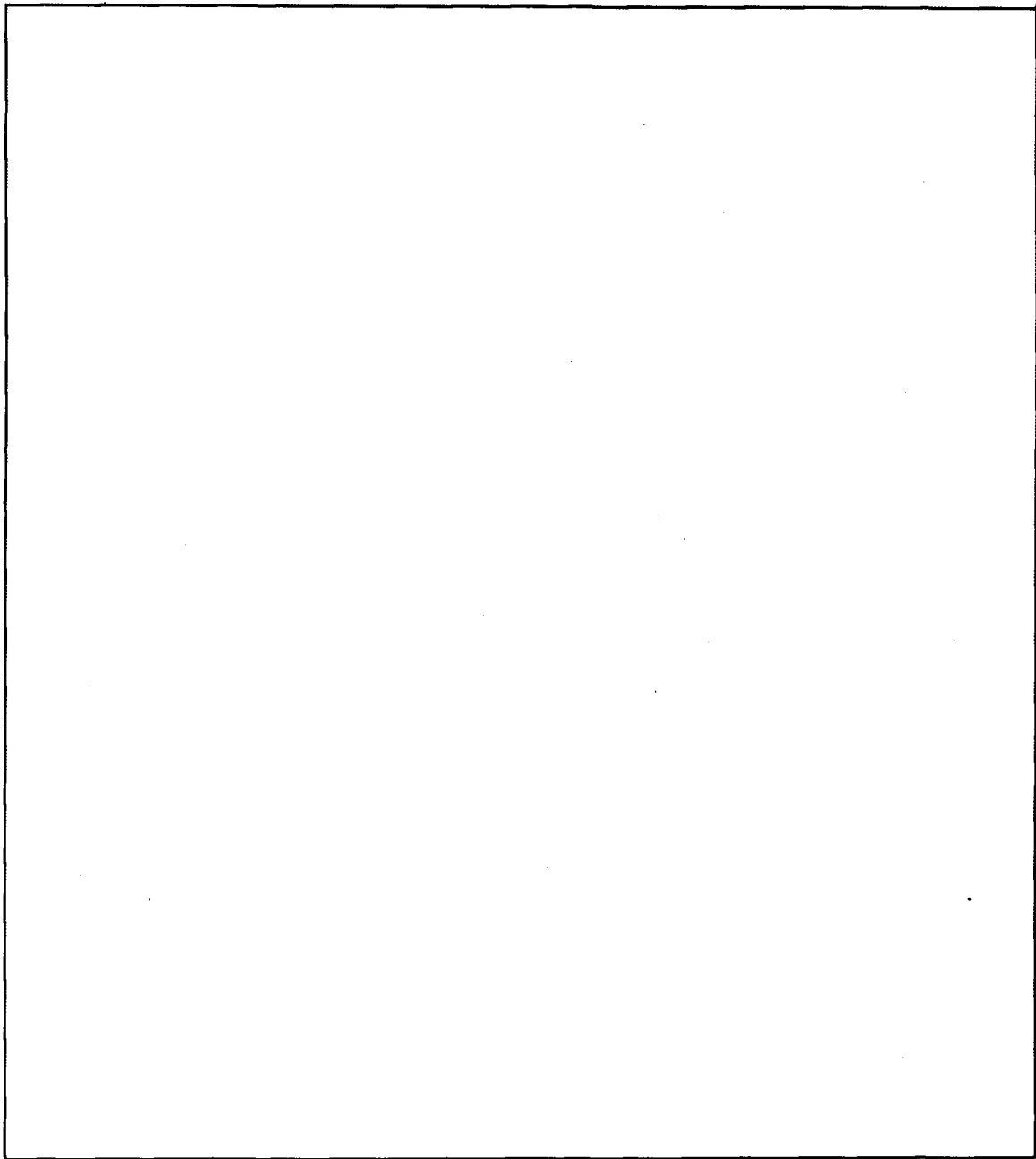


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Dedicated Process  
Controllers (U)



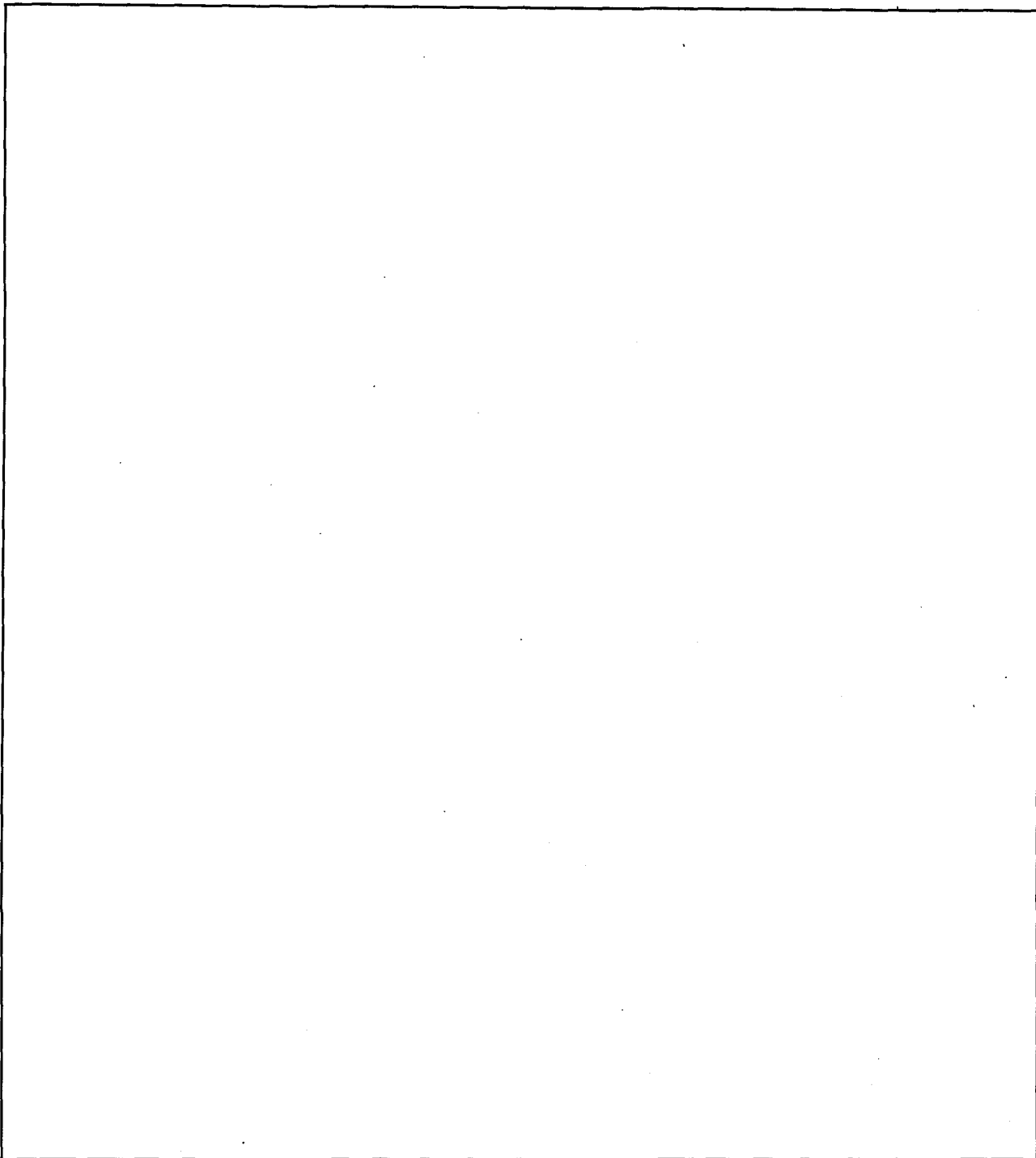
~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Dedicated Process

Controllers (U)



~~CONFIDENTIAL~~

~~CONFIDENTIAL~~\* 3. ~~(c)~~E. ~~(c)~~ DATA EXCHANGE AND DISPLAY SYSTEMS (U)

1. (U) Brief Description. A network of computers in a data exchange and display system carries out the function of accumulating and displaying common information at two or more locations. The individual computer within the system, with varying degrees of human intervention, receives digitized inputs, extracts information from these inputs, correlates them with reference data, and dynamically displays the processed information for human decision-making or other use. The same computer may transmit information and updated data to other centers in the system. Each computer site in the system may accept operator inputs by keyboard or other means which are to be transmitted to and displayed at distant sites.

Tactical data exchange and display systems make up a specialized group of this type, under which a commander is continuously provided with the latest information in his tactical environment on air defense, on air traffic control, or in other dynamic activities which he must closely follow. Computer networks serve similar functions for commanders at higher organizational levels in command and control over military forces. There are numerous other situations, including nonmilitary, in which a computer plays a part in a network for purposes of acquiring and displaying data from a continuously changing data base.

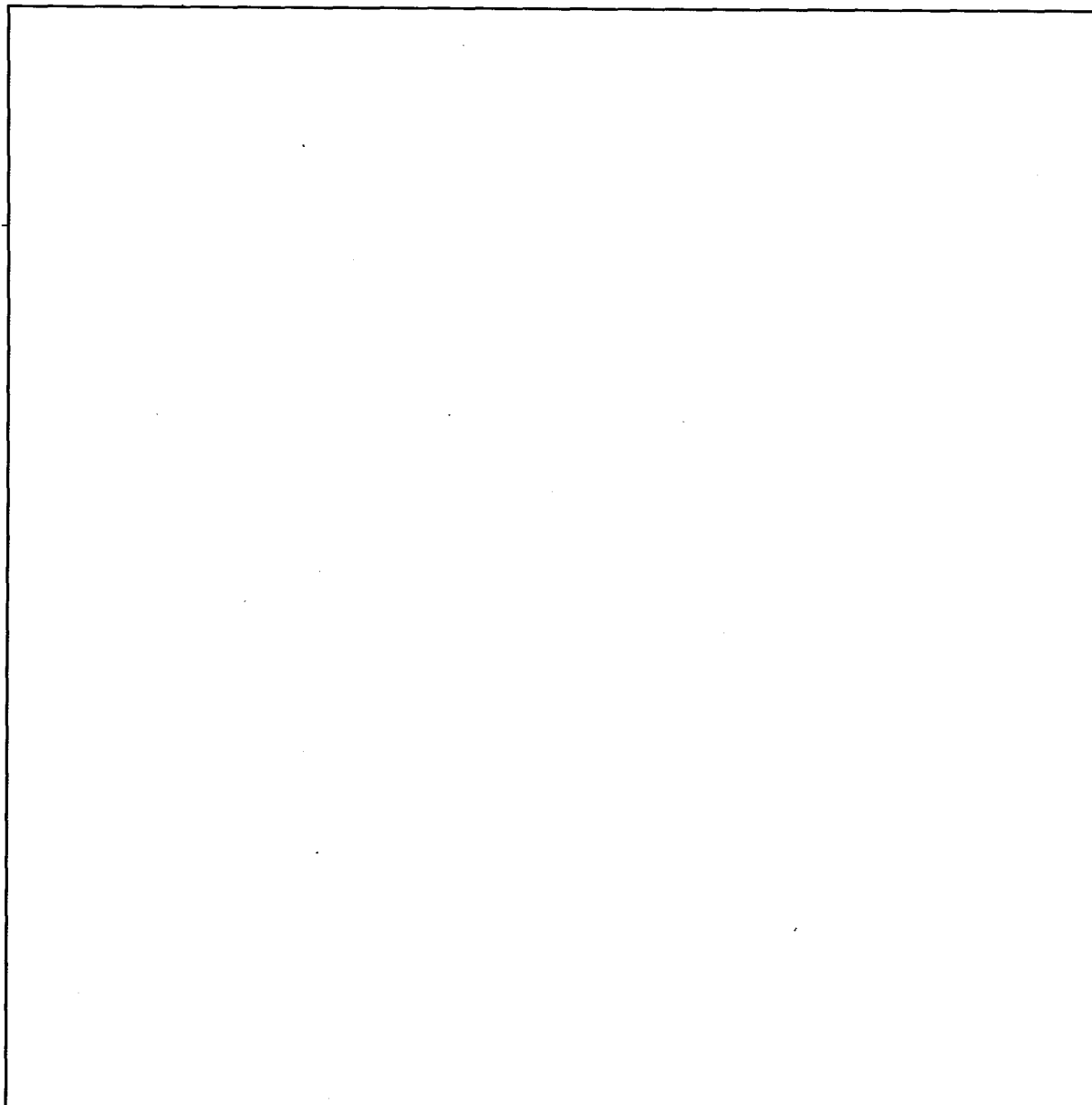
~~CONFIDENTIAL~~



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

~~CONFIDENTIAL~~

2. ~~(S)~~ Typical Threats and Countermeasures - Data Exchange and Display Systems (U)

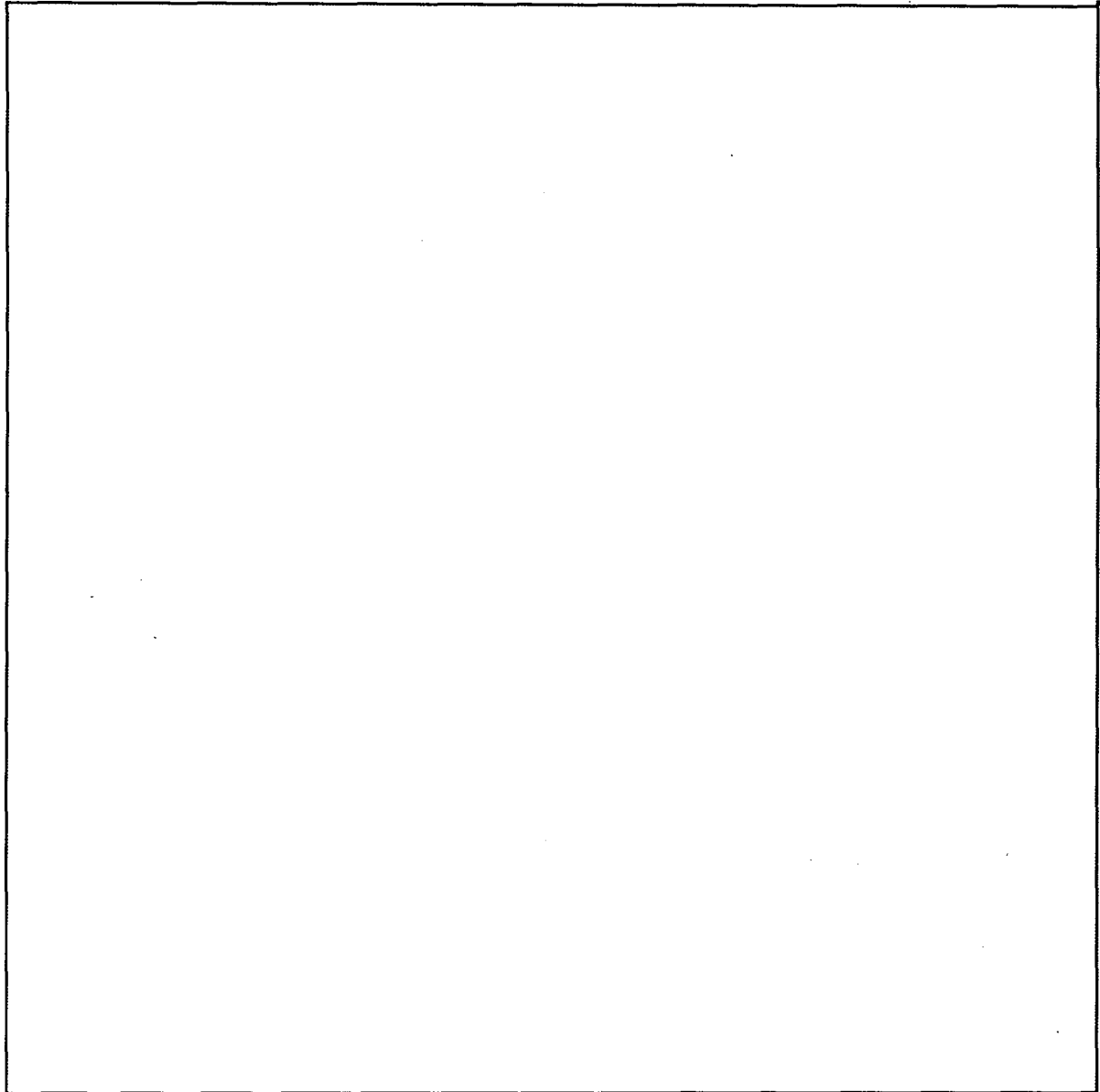


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Data Exchange and Display Systems (U)

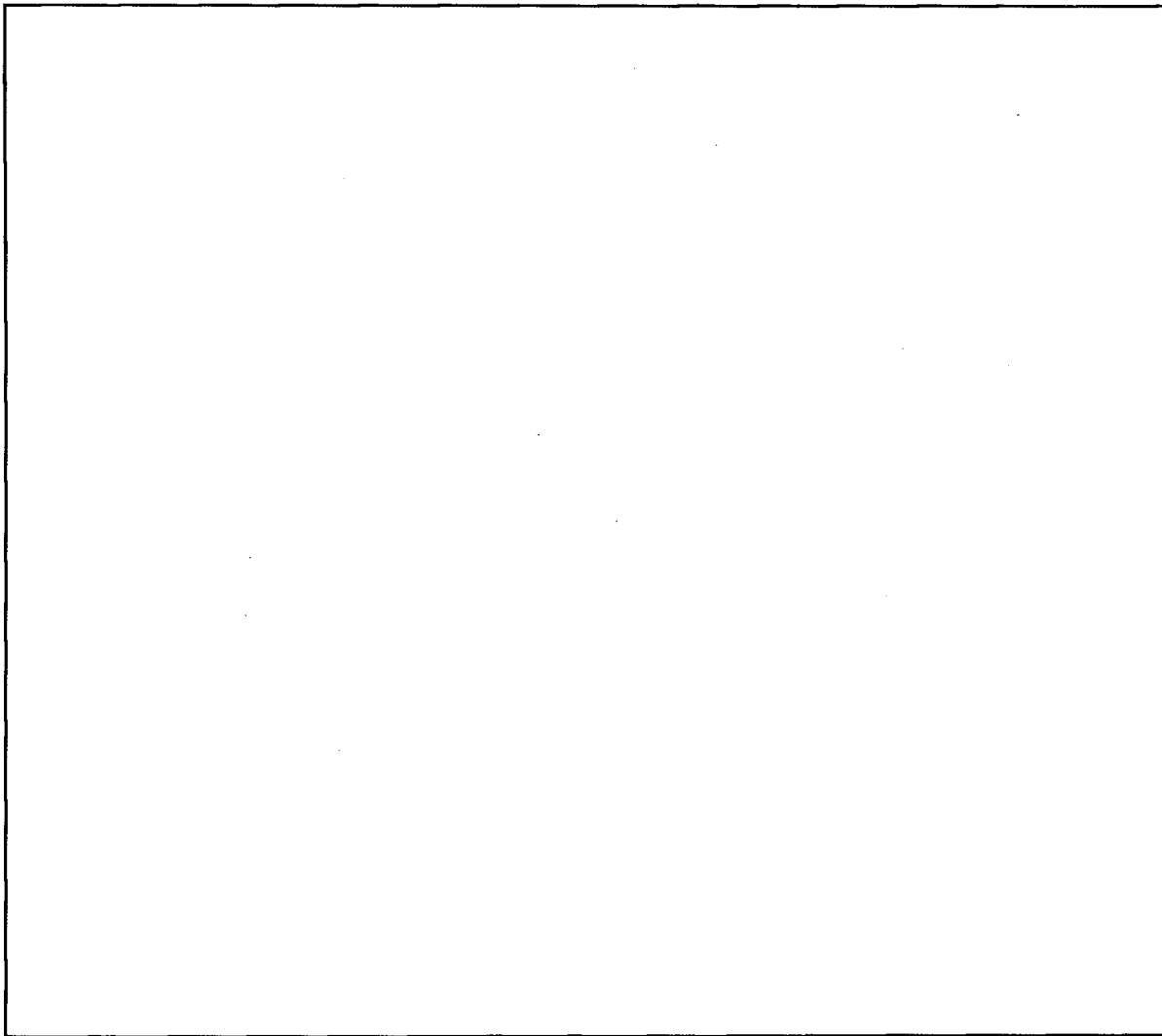


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Data Exchange and Display Systems (U)

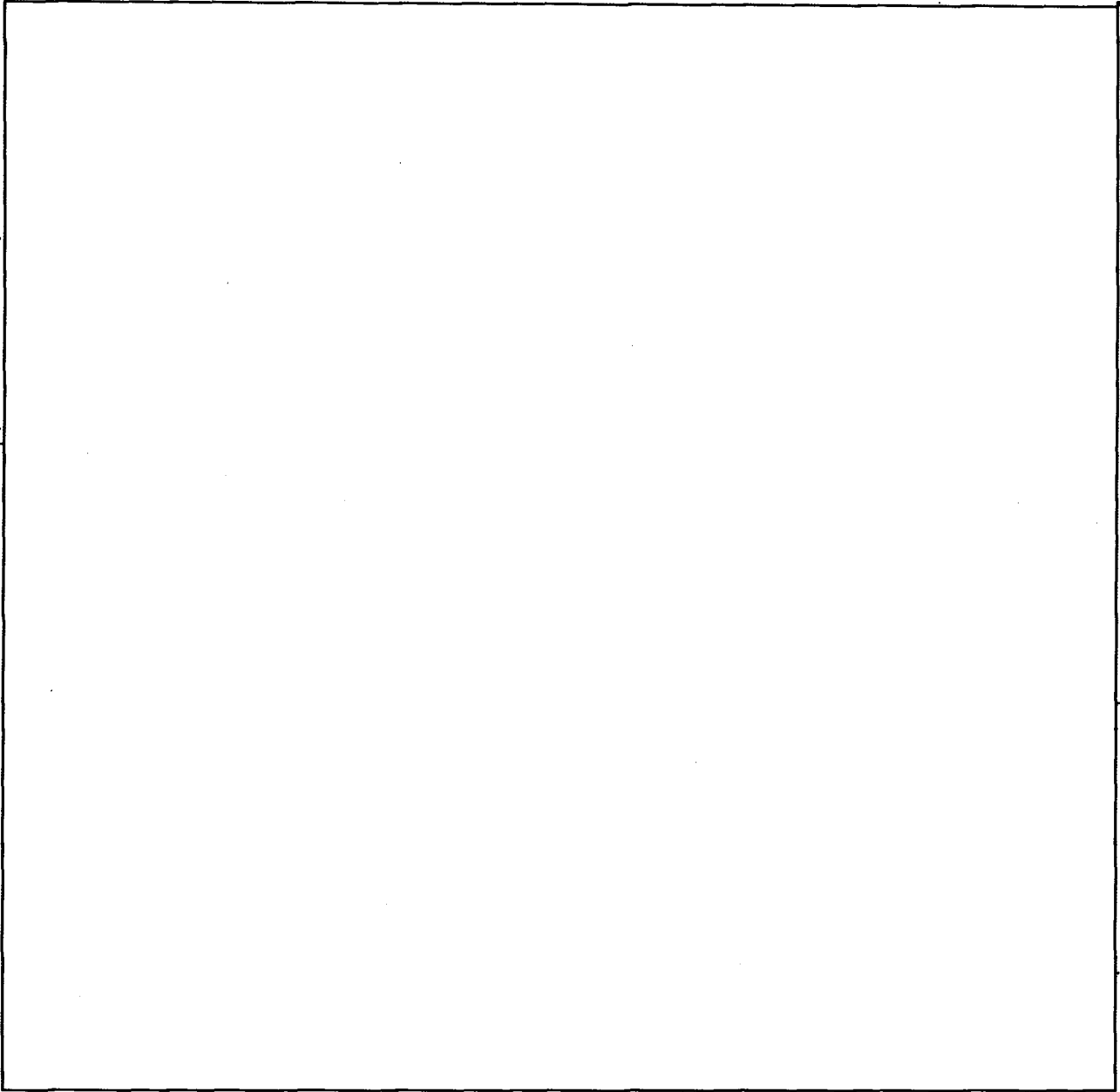


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

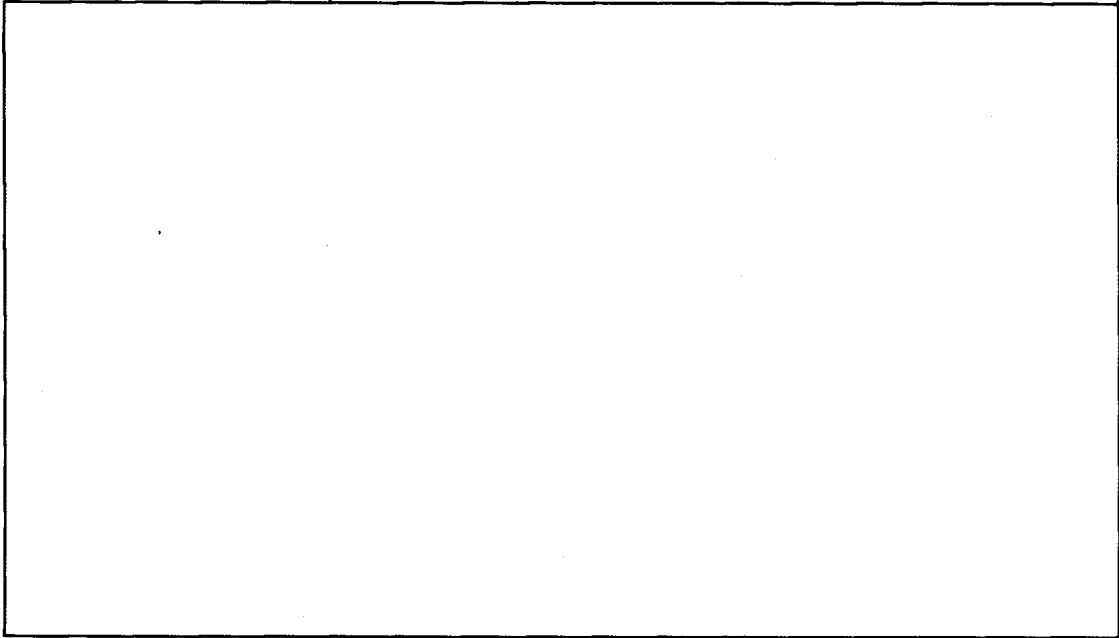
Typical Threats and Countermeasures - Data-Exchange and  
Display Systems (U)



~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Data Exchange and Display Systems (U)



\* 3. ~~(S)~~ Present Posture - Data Exchange and Display Systems. Current hardware and software technology and current design know-how permit the building of exchange and display systems which safely (at least for perishable information) process and exchange data. Security is more easily achieved and better assured when all communications links are encrypted and all terminals are monitored by personnel authorized access to entire system content. These latter constraints are an essential feature of most such systems under present protective techniques.

F. ~~(S)~~ COMPUTERS SERVING CRYPTOGRAPHIC FUNCTIONS (U)

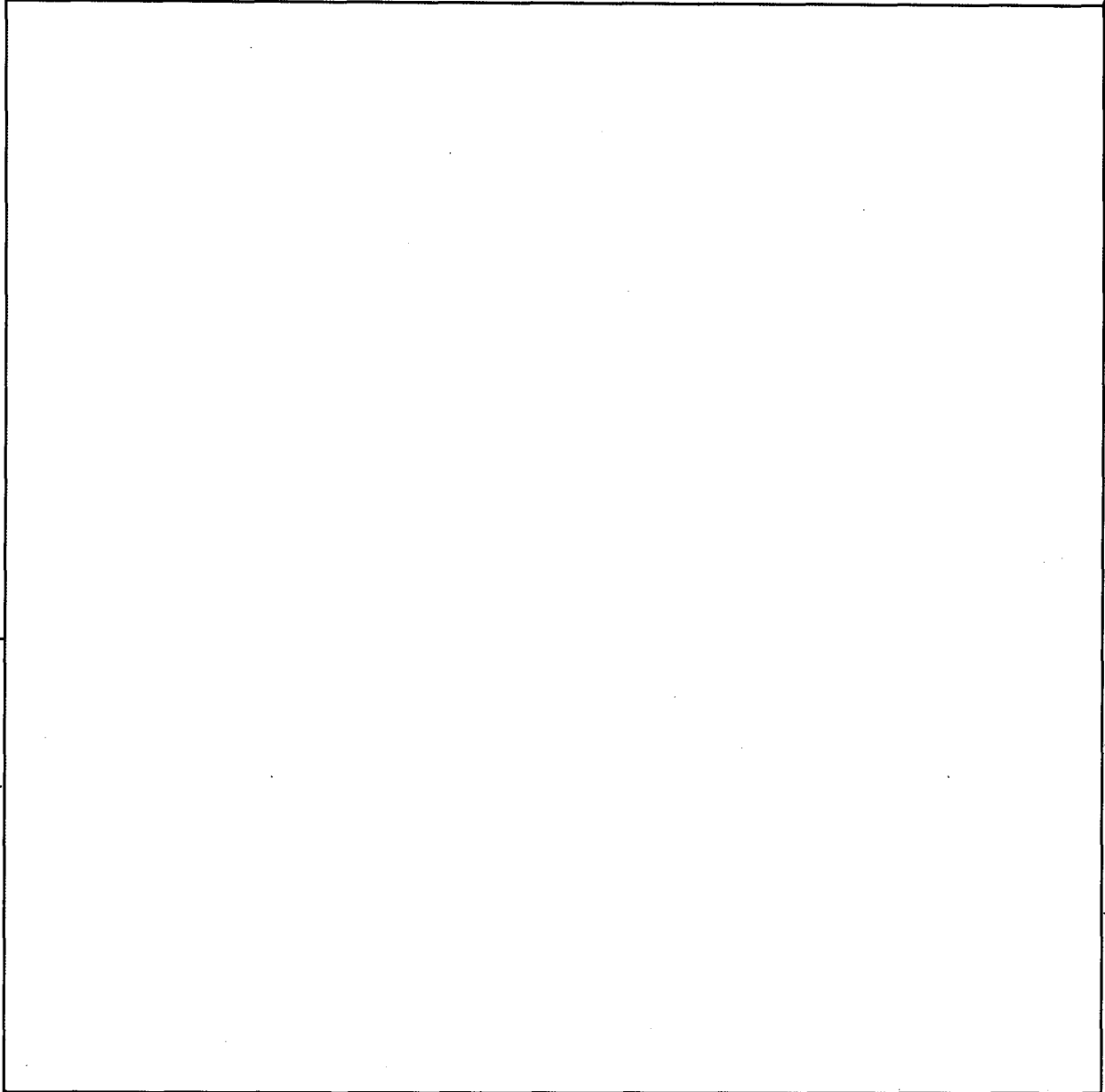
\* 1. (U) Brief Description. A computer can be used in a cryptographic system either to carry out all or part of the cryptographic function, or to control crypto-equipment or support cryptographic operation. The computer can be programmed, in software or in microcode (also known as firmware), to encrypt plain text under an algorithm designed specifically to make the most efficient use of the computer's repertoire of instructions and memory. Alternatively, the algorithm can be the same as one used in a hardware crypto-equipment. The computer can also be used to control the operation of hardware key generators. For future systems computers may be dedicated to the generation and provision of cryptovariables to crypto-equipments in the operating environment.

~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

2. ~~(S)~~ Typical Threats and Countermeasures - Computers Serving  
Cryptographic Functions (U)

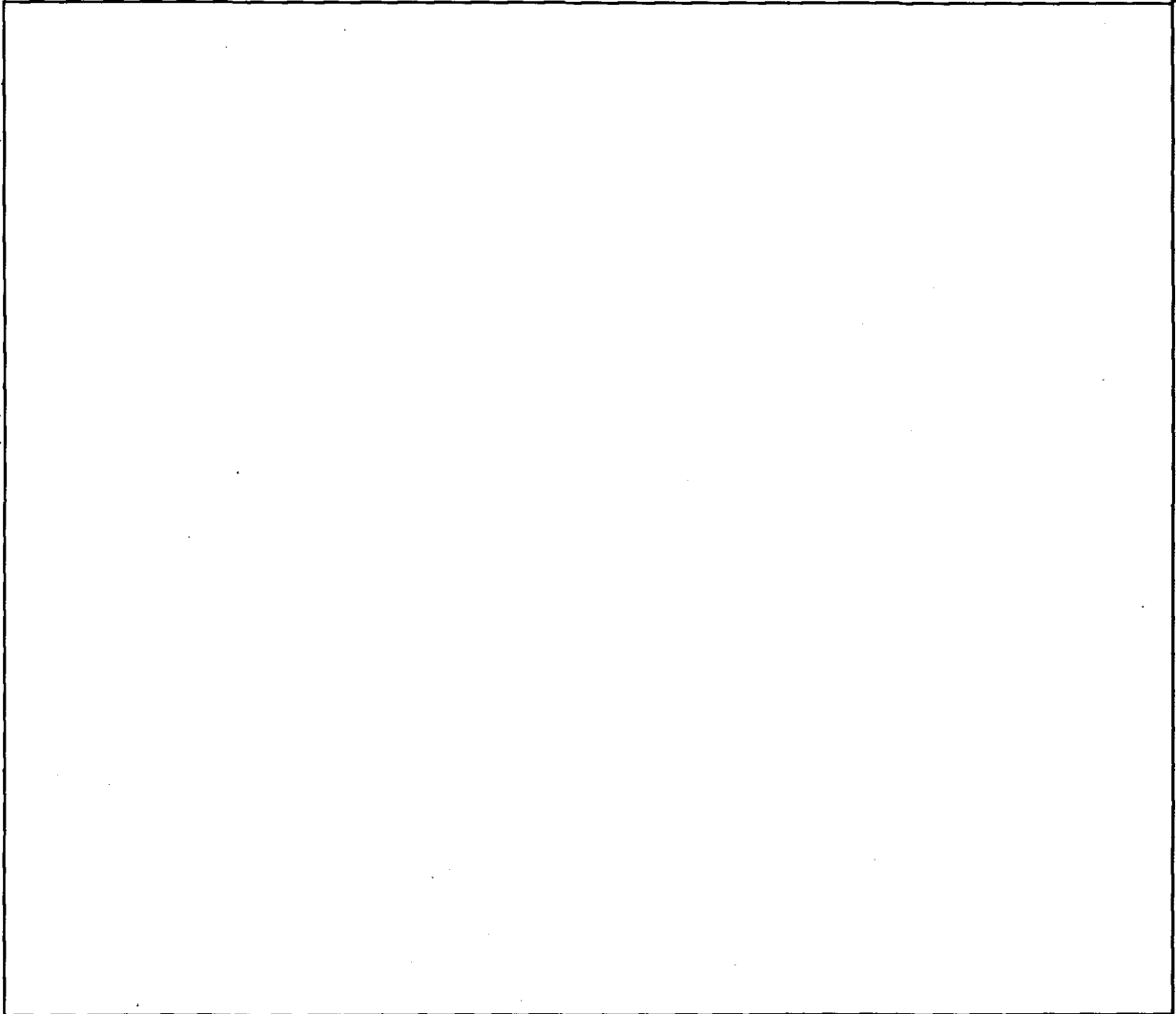


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Computers Serving  
Cryptographic Functions (U)

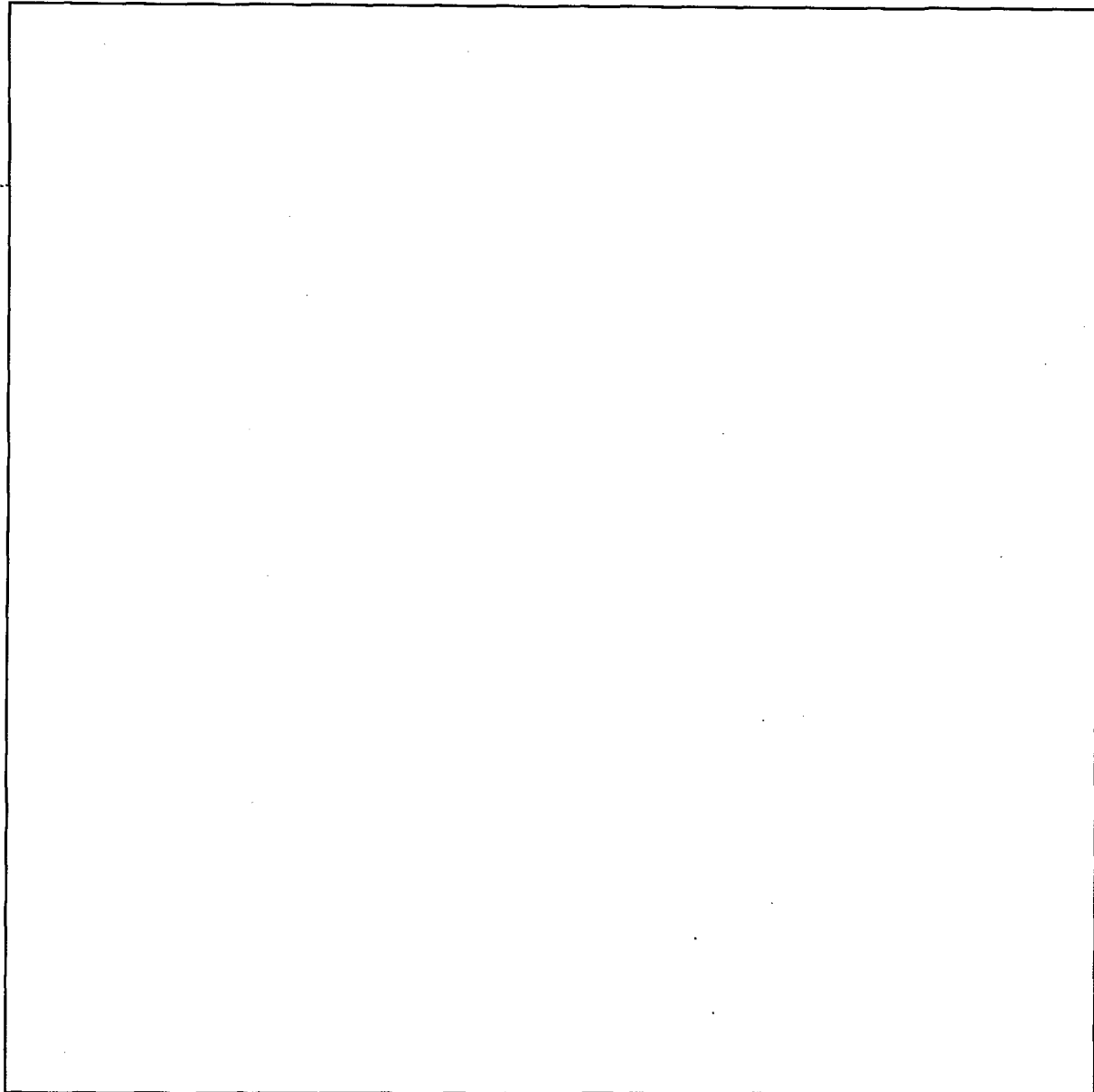


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Computers Serving  
Cryptographic Functions (U)



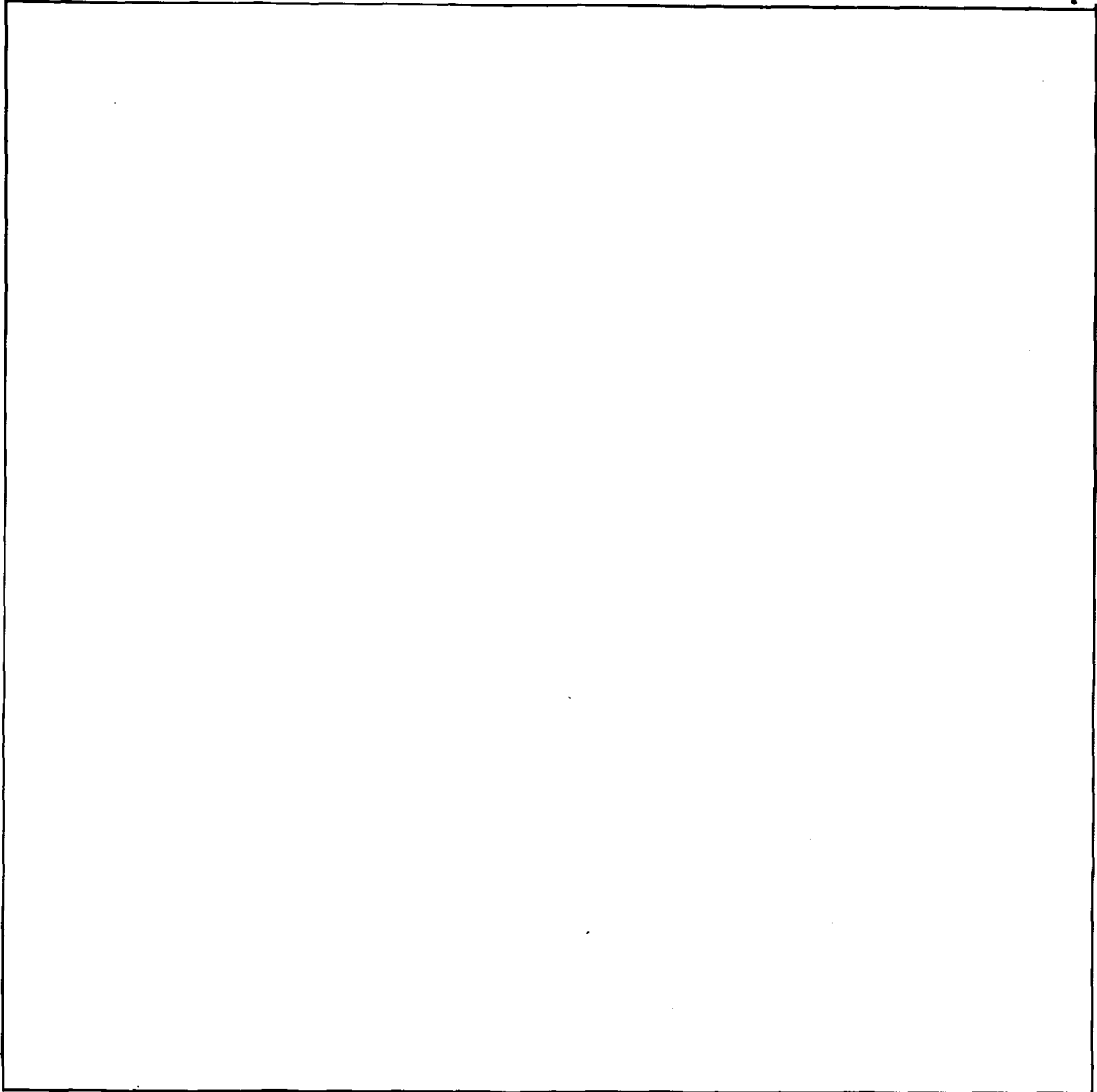
~~CONFIDENTIAL~~



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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Computers Serving  
Cryptographic Functions (U)

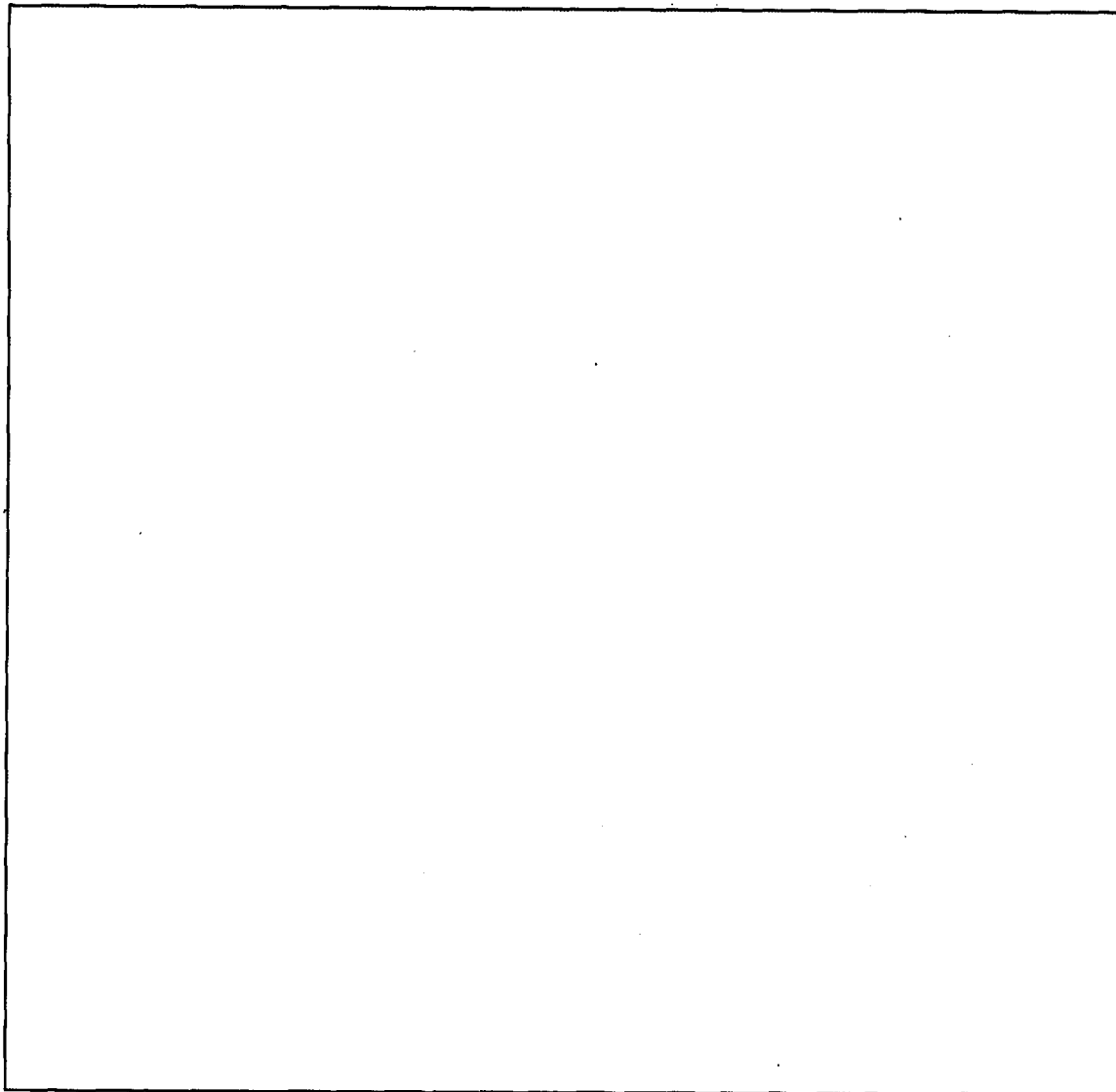


~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~

Typical Threats and Countermeasures - Computers Serving  
Cryptographic Functions (U)



~~CONFIDENTIAL~~

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

# ~~CONFIDENTIAL~~

\* 3. ~~(S)~~ Present Posture - Computers Serving Cryptographic Functions. Computers offer some possibility for carrying out cryptography in lieu of conventional cryptographic hardware; however, the techniques for carrying out cryptography within a computer have not yet been fully developed or proven. Extensive research and experimentation are necessary in order to find optimum ways to use present types of computers for encryption (and to gauge their comparative costs against hardware approaches).

\* [Redacted]

## G. ~~(S)~~ SUMMARY OF CURRENT POSTURE ON PROTECTIVE TECHNOLOGY (U)

\* 1. ~~(S)~~ [Redacted]

\* 2. ~~(S)~~ [Redacted]

3. ~~(S)~~ [Redacted]

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

~~CONFIDENTIAL~~

4. (S)

\* 5. (S)

6. (S)

\* 7. (S)

8. (S)

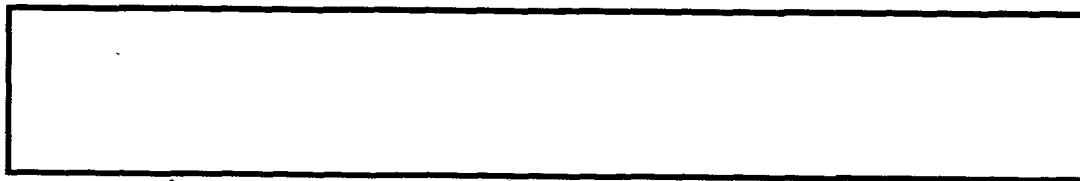
\* 9. (S)

10. (S)

~~CONFIDENTIAL~~

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

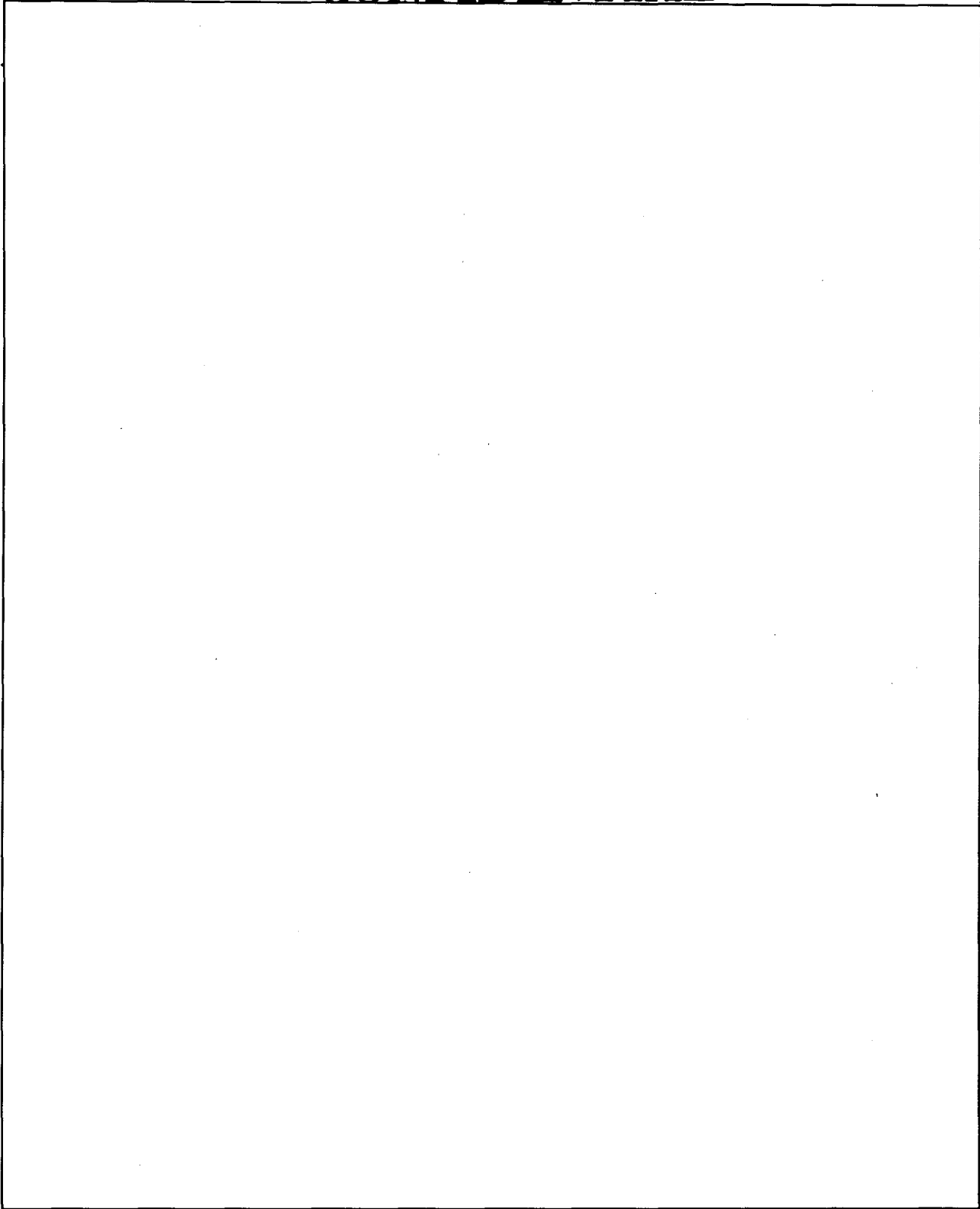
~~CONFIDENTIAL~~



<sup>50</sup>  
~~CONFIDENTIAL~~

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

~~CONFIDENTIAL~~



A-1

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~APPENDIX BREFERENCES

NAG-4A/TSEC, "Shielded Enclosures", title is UNCLASSIFIED, document is SECRET, dated September 1965.

NAG-8A/TSEC, "TEMPEST Information Memoranda-TIM", title is UNCLASSIFIED document is SECRET, dated December 1967.

NACSEM 5100, "Compromising Emanations Laboratory Test Standard, Electromagnetics", title is UNCLASSIFIED, document is CONFIDENTIAL, dated March 1974.

NACSEM 5103, "Compromising Emanations Laboratory Test Standard, Acoustics", title is UNCLASSIFIED, document is CONFIDENTIAL, dated October 1970.

NACSEM 5106, "Compromising Emanations Analysis Handbook", title is UNCLASSIFIED, Document is SECRET, dated December 1971.

NACSEM 5110, "Facility Evaluation Criteria-TEMPEST", title is UNCLASSIFIED, document is SECRET, dated July 1973.

NACSEM 5200, "Compromising Emanations Design Handbook", title is UNCLASSIFIED, document is SECRET, dated June 1973.

COMSEC ADP REFERENCES

DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems", document is UNCLASSIFIED, dated 18 December 1972.

DoD Directive 5200.28M, "ADP Security Manual".

DCID 1/16, "Security of Compartmented Computer Operations", document is CONFIDENTIAL, dated 7 January 1971.

USCSB 2-17, "Glossary of Communications Security and Emanations Security Terms", dated October 1974.

National Security Council Communications Security Directive, dated 26 August 1968.

~~CONFIDENTIAL~~

NACSEM 7002

UNCLASSIFIED UNTIL FILLED

COMMENT FORM  
FOR  
COMSEC GUIDANCE FOR ADP SYSTEMS

Use one form per comment. Return completed form to: .....

Director  
National Security Agency  
Fort George G. Meade, MD 20755

ATTN:

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

1. Date:
2. Name of Contributor:
3. Name of Organization:
4. Address of Organization:
5. Reference Section in Document:
6. Comment (What Should Be Changed?):
7. Alternative (What Should It Be Changed To?):
8. Rationale (Why Should Change Be Made?):