~~TOP SECRET~~

FIRST ANNUAL EVALUATION OF THE STATUS OF AUTOMATED INFORMATION SYSTEM SECURITY (AISS) IN THE UNITED STATES GOVERNMENT

Adopted By

The Subcommittee on Automated Information System Security

7 February, 1985

25X1

[redacted]

25X1

[redacted]

[redacted]

25X1

~~TOP SECRET~~

NSA CONTL. NO. 8500646
COPY NUMBER 25
THIS DOCUMENT CONTAINS 21 PAGES

TABLE OF CONTENTS

PART I - INTRODUCTION

PART II - ASSESSMENTS

PART III - RECOMMENDATIONS

APPENDICIES

25X1

UNCLASSIFIED

EXECUTIVE SUMMARY

The overall Automated Information Systems Security (AISS) posture of the United States Government has been poor and rapidly getting worse. The signing of the National Security Decision Directive 145 (NSDD 145) now puts the government in a position to bring fragmented policy, procedures, tools, mechanisms and techniques into line with the advanced technology of today and the expanding role of AISS in the government. The present fragmented, and sometimes inconsistent, approach that the government has taken to protect its automated information systems resources has been allowing our adversaries, both foreign and domestic, to increasingly benefit from these resources. If we can correct the deficiences as noted below and implement a more cohesive approach to securing these valuable resources, then both near-term and long-term benefits can be reaped.

The Subcommittee on Automated Information Systems Security (SAISS) found that there is no coherent, uniform policy for Government departments and agencies, nor is there a uniform approach as to what computer security programs should encompass. Each agency funds computer security measures separately and differently. Such variation, attributed in part to the multiplicity of policy flowing from various sources through different channels to affected departments and agencies, hampers a cohesive approach to overall resource for and programmatic management of computer security, even within agencies. Furthermore, the SAISS determined that one reason that there are not more secure products and systems available is that there is no government-wide policy mandating their use.

The use of automated information systems is becoming more widespread to the extent that it is almost impossible to identify requirements that do not rely on computers for some, if not all, of their information processing and protection needs. Future technologies, particularly the growth of desktop computers, the increased local storage of data and the widespread networking, will exacerbate existing security vulnerabilities as well as create new ones. As this technology has grown, the resources and awareness needed to allow security technology to grow with it have not kept pace. The use of traditional COMSEC, physical security, personnel security and administrative security protection techniques does not sufficiently protect the type of information sharing that is becoming increasingly common in new automated information systems, especially distributed processing and networked systems.

UNCLASSIFIED

There is a wide spectrum of threats to and exploitations of the Government's computers from hackers, hostile intelligence services, terrorists, criminals, and even properly cleared people with no need-to-know. The SAISS found evidence that even the extent of the problem is not completely known because there are insufficient tools in most systems today to accurately record the usage of automated information systems. Threats to and exploitations of automated information systems exist at all points where there is unrestricted access.

Although the vulnerabilities are relatively well understood, existing measures to counteract them are not uniformly and consistently followed. Because there is not a policy mandating the use of secure products and systems, there are major voids in the area of technical (software and hardware) protection mechanisms and products that could allow the government to achieve significant gains in the protection of automated information systems.

However, significant gains can be seen by the formation of the DoD Computer Security Center (the Center) and the subsequent establishment of the Computer Security Evaluation criteria and the formal evaluation process, the promulgation of the NSDD-145, the Intelligence Community Computer Security Project, the work of the Interagency Group/Countermeasures and establishment of the DOE's Computer Security Center.

The major conclusion of the SAISS, based on existing government information sources, is that the government does not know the extent to which it depends on automated information systems and, therefore, a quantitative assessment of its relative security cannot be made in this first annual evaluation. However, there is a common theme in the existing data from which the following major deficiences have been extracted: 1) while adequate auditing, detection, and other administrative control procedures could currently be used to improve the protection of existing systems (and their use is mandated by such diverse policies as OMB Circular A-71, TM-1, and others) such protection mechanisms are not implemented consistently and there are insufficient resources to use them effectively; 2) the full extent of the threat to and vulnerabilities of automated information systems is unknown; 3) the goals of automated information systems productivity and automated information systems security are often erroneously perceived as mutually exclusive; 4) the trend to networking and distributed processing is adding to the overall AISS problem; 5) there is a major need for a National AISS Awareness program; 6) most automated information systems that are embedded in other functional systems are not adequately covered with respect to continuity of operation; and 7) there is a need for more research, development, and implementation of technical AISS and COMSEC measures which can support AISS.

To alleviate these deficiencies, the SAISS recommends that the Systems Security Steering Group (SSSG) task the National Telecommunications and Information Systems Security Committee (NTISSC) and/or the SAISS to take immediate action to begin implementation of the near- and long-term recommendations. In particular, the mechanisms by which a yearly assessment of the status of automated information systems in the government should be established and implemented. Although there are many recommendations that can be implemented in the next year at little or no cost, to achieve the substantial long-term gains needed to address the AISS problem, additional resources (budgetary, personnel, and technical) will be required.

I. (U) INTRODUCTION

A. Purpose of Report

This report is the first annual evaluation of the state of Automated Information Systems Security (AISS) in the United States Government. It is intended to be combined with a similar report on Telecommunications Security and sent to the Systems Security Steering Group (SSSG), who will then make recommendations to the President's National Security Advisor.

B. Authority

This report is produced on the authority of the National Security Decision Directive 145 (NSDD 145) that requires an annual evaluation of the status with respect to established objectives and priorities of AISS and Telecommunications Security by the National Telecommunications and Information Systems Security Committee (NTISSC) and submitted to the Systems Security Steering Group.

C. Sources

Inputs from members of the working group of the Subcommittee for Automated Information Systems Security (SAISS) were assembled to prepare this report, see APPENDICES B and C.

II. (U) ASSESSMENT

A. (U) Policy

1. It is apparent that there are a large number of computer security policy documents in the Government which assign responsibilities for protection of classified and unclassified information. These policies and the organizational structures established to execute them derive from a number of authoritative sources which have different purposes.

2. According to the recent report of the Policy Survey Subcommittee chaired by OSD, at the request of the NCSC, entitled Survey of Federal Computer Security Policies, there are over 32 separate computer security policy documents in the 15 agencies surveyed. Although only 15 agencies were surveyed, these together accounted for over 88% of the government systems in the GSA ADPE Inventory. These policy documents varied substantially in approach, scope, and applicability. This variance, in turn, can result in the perhaps unnecessary imposition of multiple and conflicting requirements on systems concurrently processing multiple information categories subject to such policies. A closer viewing would probably show that most of these documents do not, in fact, address the most current technology environment, e.g., networks. (See APPENDIX A for list of some of these policies.)

3. Virtually every agency of the Government processes sensitive information on a daily basis. A cohesive and integrated policy is necessary since the trend toward networking of resources has fundamentally altered the scope and nature of the security issues to be solved. One of the key areas where the Government lags behind is in policy development, promulgation, and implementation.

B. (U) Assumptions/Trends

1. The Government now owns or operates in excess of 20,000 mainframe computers processing vast quantities of classified and sensitive information which is vital to the national security interest of the United States, thus increasing the potential for security leaks and the opportunity for access to and modification of data by users having hostile intent. 'Embedded' computer systems have been projected by an industry group to grow within the DoD from about 10,000 in 1980 to 250,000 in 1990. As storage costs decrease, the amount of data stored at the mainframes increases, creating more appealing targets. As networking expands, more and more users will have potential access to a broader range of information. It is possible to aggregate sensitive government information given large bodies of information on the same or related topics even if the entire collection of data is unclassified. As end users of computers continue to increase their technical competence and computer literacy, the technical and management AISS task of protecting data and controlling users has fallen even further behind.

2. The dependence on computers to support mission requirements has increased and will continue to increase, as has the number of powerful personal computers. There is also more demand for interoperability, interconnectivity, and distributed processing. This is rapidly leading to: more data and more diverse data, more information exchange, and increased reliance by management on computers. Programs for protection of these information resources have not kept up with the application of such systems, the growth thereof, or technology advances for a number of reasons, such as, lack of sufficient high-level management emphasis, lack of resources (both manpower and funding), and lack of supporting AISS technology; the market place has not demanded that developers and vendors of new systems (hardware and software) provide control and protection hand-in-hand with functionality and connectivity.

3. Information gleaned from various security policy documents and inputs from the SAISS members indicated that the lack of a uniform policy regarding sharing and protection of information by several agencies/departments creates an impediment to AISS. For example, when one agency sends sensitive information to another agency, there are few common guidelines on

how this information should be protected. As a result, the actual receiver or custodian of the data is the one who determines the protection to be provided and/or the handling.

4. The overall state of computer security R&D within the government is weak and getting weaker. Since the capability of the government's adversaries is constantly improving and since the government continues to compound its risk by pursuing more and more interconnectivity, the risk of penetration and of subversion increases. Security must focus on both near-term and long-term issues. While R&D provides answers to the long-term issue, the Government must take immediate action to close the security gap and reduce this risk by encouraging the developing of products which offer greater resistance to malicious attack. It will take an active and aggressive U.S. Government R&D program coupled with improvements in physical, personnel, and administrative security features and an enhanced certification program to effectively enhance the overall effort of strengthening the computer security of automated systems.

5. The recent DoDCSC survey, Survey of Automated Information Systems Security, within the DoD establishment revealed that 62% of classified systems established to operate in the dedicated mode are operating in such a way as to lead to a high risk of compromise of information. The survey results are an indication that policy is not well understood, is misapplied, or else is being ignored. Computer security policies government-wide need to be revised to address consistently the increasing threat and reduce identified vulnerabilities.

6. There are traditionally three different aspects to computer security as perceived in the government today. The first of these aspects is "protection of information from compromise" and is the principal topic of concern in civilian, intelligence and military directives. The directives basically state that information should be revealed to persons who have the proper clearance and need-to-know. The second aspect deals with "integrity of information", i.e., that the information is not be modified nor changed in any way; this aspect is most often associated with the financial and military command and control communities. The third aspect is not strictly a security issue in the classical sense, but nonetheless a real concern, i.e., "denial-of-service": "Will the automated information system be there, operating as planned, when it is needed, or will it be unavailable due to computer hacker, terrorists, etc?" Various elements within the government are concerned to varying degrees with each one of these different aspects.

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP97M00248R000500170013-4

Page Denied

Next 2 Page(s) In Document Denied

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP97M00248R000500170013-4

5. (U) Authorized Personnel

a. A majority of the crimes committed against government systems are by persons internal to the organization. The potential for damage from the disgruntled employee is enormous, since he in most cases has not only the motivation for causing harm, but also the detailed knowledge which can make enormous damage possible. According to the report of the President's Council on Integrity and Efficiency (PCIE), the total of losses PER EVENT from fraud and abuse in these types of situations was over $185,000.

b. Another threat to government automated information systems is from the results of legitimate mistakes which do occur. These mistakes have the potential of creating large losses of time, resources, etc. Systems with a high degree of security, and trustworthiness, coupled with good software engineering and quality assurance practices will help to overcome the severity of losses due to this threat. An example of this type of threat would be a mistyped instruction in an unprotected system which might allow erasure of some other user's data. Though we would caution that good computer security features cannot cover up weak management practices vis-'a-vis software engineering and quality assurance.

D. (U) Vulnerabilities

1. (U) This section describes the vulnerabilities of computer systems in use by the government. The emphasis in this section is not so much on specific systems and their specific vulnerabilities, but rather on typical systems and vulnerabilities that exist today. To address specific problems could lead to the false hope that if fixed, the vulnerability problem would be adequately solved in all general applications.

2. (U) Computer security vulnerabilities are in all of the areas associated with the protection of information. These various protection mechanisms are: 1) physical; 2) personnel; 3) administrative/procedural; 4) communications/emanations, and 5) hardware/software internal to a computer system. The vulnerabilities in areas 1, 2, 3, and 4 are relatively well understood and there are existing protection mechanisms which, if used properly and consistently, are effective though many agencies of the government still need to make significant improvements in these areas. However, it is in area number 5, vulnerabilities to the hardware/software mechanisms where continued attention to major development is needed. The significance of these vulnerabilities has two dimensions: first, it impacts the reliability and effectiveness of security functions implemented within a multi-user system as such; secondly, it impacts the overall system security posture and its accreditation, since hardware/software security and the other cited protection areas

25X1

Page Denied

Next 2 Page(s) In Document Denied

Board is addressing the issue of the continuity of operations of a full spectrum of public and private NSEP functions which depend upon uninterrupted automated information system's availability.

7. Congress passed the first federal computer related crime bill (P.L 98-743), "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984." This bill prohibits unauthorized access or abuse of authorized access to a computer for any of three unlawful purposes: a) to obtain national security informaiton (a felony); b) to obtain Financial Privacy Act protected information or Fair Credit Reporting Act protected information (a misdemeanor); or c) to modify, destroy or disclose information in a computer or to prevent authorized access to the computer when the computer is operated by or on behalf of the U.S. (a misdemeanor).

F. (U) Conclusions

1. The current collective efforts, (including policy, organizational and programmatic aspects, definitions and standards) designed to ensure adequate protection of automated information systems and networks appear to be inadequate. Current programs clearly will not effectively keep pace with the anticipated expansion of computer/network utilization projected in the balance of the 1980's and beyond.

2. The full scope of computer-related fraud and abuse in the government is still not known. The fact that most agencies do not systematically distinguish computer-related cases from other types of white-collar crime in their case tracking systems contributes to this situation. However, the major reason is the non-existence of a workable system for detecting these crimes. Those available internal audit, detection, and control mechanisms are not in widespread use either due to a lack of understanding of their importance, cumbersomeness of the systems, or a lack of resources to carry them out to the degree required. Reports from the Air Force Office of Special Investigations (AFOSI) suggest that three fourths of the perpetrators of either fraud or abuse cases acted alone, aided by the lack of management and accounting controls.

3. Despite the possibility of a greater availability of technical computer security features, the fragmentation of present computer security policy is hindering the improvement of AISS in the federal government and if all remains as it is today, the posture is likely to get worse. Also, because of the lack of any clear policy mandating the use of trusted products and the absence of a successful strategy for promoting the availability of trusted products, the market for such is limited. The heads of Government departments and agencies are likely to continue to

ignore computer security standards and guidelines unless computer security responsibilities are clearly delineated and the use of available computer security products is mandated by policy.

4. Most systems that are in use today, especially systems that are dedicated to some specific function (e.g., the national telecommunications network) do not have adequate continuity of operations plans or facilities. Disruptions or outages (due to terrorist attacks, hostile action) would cause considerable, and in some cases unrecoverable damages. Indeed, some critical operations are now so highly automated that to fall-back to the original "manual" operation is no longer feasible or possible. Further, no current program to specifically ensure the availability of data in a national emergency or crisis exists.

5. There is a clear trend toward distributed processing and networking of resources. Yet, there is very little existing AISS policy and guidance for the internetting of the systems. The need for network security policy and guidance is further reinforced by on-going acquisition and expected future massive growth in microcomputers (e.g., "desk-top" and "personal" computers) and in local area networks. The complexity of systems has made the successful inclusion and analysis of security features more difficult. Policy is needed to ensure comprehensive and continuing security of sensitive information and applications processed by word processing systems, microcomputers, local area networks and other computer-driven information systems not commonly designated "ADP systems". Such systems are not explicitly covered by existing policies; however, the systems are not radically different insofar as needed security actions and approaches are concerned.

6. Awareness, especially on the part of management, of the current and projected vulnerability and risk dictating a need for increased security is seriously lacking. Support by the Government's top management and senior executives concerning the recognition for AISS and the role that AISS can play in assuring the security of the Government's mission is insufficient. More often than not, decisions are made to process sensitive information without a clear understanding on the part of senior managers of the security risks that are associated with processing such information within a specified computer architecture. Generally, such decisions to process data are being made at a fairly low management level. Contributing to the vulnerabilities is the uneducated and unfounded widespread resistance to expend scarce resources for an unquantifiable gain from the use of computer security protection mechanisms and/or secure products. An erroneous assumption by a majority of Government managers is that computer security exists in an "either/or" relationship to computer efficiency and productivity. Unfortunately more

misguided emphasis is being placed on productivity at the expense of demanding more secure products. However, good computer security is inherent and integral to good system design.

7. Use of security procedures, mechanisms, and controls which are available at present is not widespread. Waiting on new R&D technology to improve the AISS posture is not always required.

III. (U) RECOMMENDATIONS

A. Policy

1. The SAISS should be tasked by the NTISSC to look at the aggregate national-level policy fragmentation situation and explore the feasibility of a responsive uniform and comprehensive national AISS policy framework.

2. In particular, the SAISS should be tasked to develop and formulate, for issuance by the Executive Agent, policies:

a. For the identification of government and non-government sensitive systems.

b. For the identification of the critical systems of the Government and of the Private Sector.

c. For Uniform and Broadly Applicable AISS Standards which include some notion of mandatory and discretionary access.

d. For the Continuity and Useability of Critical Systems.

e. For a policy model for the sharing of sensitive and classified data.

f. For mandatory computer security considerations supported by manadatory risk management during the development and procurement cycles.

g. For a mandatory, uniform, and broadly applicable survey for assessing the status of AISS and network security in the government.

h. For a National Computer Security Awareness Program.

i. For a National Computer Security Training Program.

UNCLASSIFIED

3. Establish policy such that heads of Departments and Agencies should provide the mechanisms to apply appropriate resources to upgrade the security of automated systems under their purview and provide summaries of such actions as an input to this annual report on the status of automated information systems in the Federal Government.

B. Near-Term Recommendations

The following recommendations can be implemented in the near term and will yield significant security benefits relative to the minimal cost of implementation. These recommendations can all be implemented with the technology and mechanisms that are available today. The SAISS should be tasked to develop the policies and/or directives whereby these recommendations are made mandatory implementations for the Government's classified and sensitive systems within the next 36 months.

1. Require a Security Officer for each multi-user automated information system and each network. All computer systems and networks that process infor-mation that is sensitive (from privacy to the most sensitive national security information) should have associated with them an information/computer System Security Officer (SSO). This officer should have delegated to him from the highest levels of management the authority to ensure that adequate security mechanisms are available for that system and that they are used consistently.

2. Implement an interim security awareness program until a national policy/program can be implemented. Each department and agency should forthwith implement a security awareness program that has visible top management participation and which instructs the individual about his personal computer security responsibilities and accountabilities and which includes the following good computer security practices:

a. Require a written system security plan for all U.S. Government computer systems and networks processing sensitve or classified information.

b. Require personal identification and authentication for each multi-user automated information system. All systems should be operated in such a manner that each user has a unique login name to identify himself to the system and a password to provide authentication. This mechanism will ensure that no group accounts exists for any system, application, or maintenance functions.

UNCLASSIFIED

c. Require audit trails (by individual user/process) for all multi-user systems. Detailed records of all security-related uses of the system should be kept by the system. This mandatory record of all users of the system should be reviewed by the security officer on a daily basis so that any security problems can be dealt with promptly.

d. Enforce the use of controls on the physical access to the multi-user computer room/area. A daily log of the physical entry by all individuals to the computer room should be kept and reviewed by the SSO. For systems processing classified, sensitive, financial and/or personal data, controlled access procedures should be mandatory.

e. Enforce the use of security restrictions and controls on removable storage media. Each department and agency should implement a security management program to control the removal and introduction of removable storage media from/to its facilities.

C. Near-Term NTISS Issuances
(initiatives started within the next 12 months)

1. The Director, Computer Security Center should be tasked to provide a schedule for the development and formulation of NTISSC Issuances on the following subjects (though not limited to the list).

a. Data Remanence

b. Environment Guideline

c. Vulnerability Reporting Program

d. Trusted Computer System Evaluation Criteria

e. Guidelines on Password Management

f. Model Password System

g. Audit Guidelines

h. Discretionary Access Control

i. Network Security Criteria

j. Guidelines on Office Automation Security

k. Procurement Guidelines for Specifying Levels of Computer Security Trustworthiness.

l. Guidelines for the development of systems security plans.

UNCLASSIFIED

D. Long-Term Recommendations

1. Foster the development in industy of additional automated tools, equipments, systems, and techniques to minimize reliance on manual techniques for security. Because the Government represents only a small portion of the market, industry will continue to move slowly in the development of computer security mechanisms until the business community expresses a demand for these products. Government must strive to seek new relationships with industry, including joint ventures between the two, in order to develop a full range of trusted computer security products.

2. Provide a superior technical base within the government on computer security issues, principles, and practices. Develop individual R&D centers of expertise as a way to build up this base. As a last resort, the Government might have to take a direct approach and detach itself from a total dependency on industry and develop those products that are urgently needed now to protect many applications against software and hardware subversion.

3. Encourage and support a superior technology base within the private sector for the design of commercially available computer systems with enhanced security properties. As a beginning, the products might have to be developed under Government sponsorship in an unclassified environment or possibly in a classified environment with industry funded development.

4. Encourage and support more research in providing security to networks of computers.

5. Encourage and support more transfer of technology to the private sector to enable it to supply additional computer systems with enhanced security features, e.g., access control mechanisms, to the government.

6. The Executive Agent should direct the Computer Security Center to identify the resources required to evaluate at least 25 of the major hardware and/or software configurations used by Federal Government automated systems (e.g., Model 204, Inquire, CIA GUARD, FORSCOM GUARD, LSI GUARD, KAIS GUARD). The objective of these evaluations should be to expand the Center's Evaluated Products List to approximately 30 products by the end of FY86. Such an action would provide a more systematic approach to the evaluation of the security of automated systems in the Federal Government.

7. Computer security programs are based on the fundamental premise that automated systems cannot operate in a totally risk-free environment. Risks must therefore be managed.

UNCLASSIFIED

Officials in their roll as risk managers must accomplish a series of actions to assure risk management plans are comprehensive and usable. Actions for management consideration are: (1) define the risk environment: review and document current and proposed hardware, software, and facilities; (2) define risk categories: identify and document threats to, and vulnerabilities of, the automated system environment; (3) evaluate risk occurrence: documented risks should be associated with likelihood for occurrence; (4) identify risk impack: calculate damage should the risk materialize; (5) idenfity risk reduction decisions: risk reduction decisions should be documented, safeguards selected for implementation, budgetary limitations and plans should be included; (6) develop a risk reduciton plan; (7) implement the controls; (8) develop a risk reduction maintenance plan; and (9) review and audit the risk management plan.

UNCLASSIFIED

APPENDIX A

POLICIES AND AUTHORITIES

1. Executive Order 12356
2. Special Access Programs for Intelligence (E.O. 12333, DCID No. 1/16)

3. National Communication Security Directive

4. Executive Order 10865 "Safeguarding Classified Information within Industry."

5. Executive Order 12333.

6. Atomic Energy Act of 1954. Authority for unclassified information include the following documents.

(1) Privacy Act of 1974 and OMB Circular A-10i

(2) Transmittal Memorandum No. 1 to OMB Circular A-71.

(3) Records exempt from disclosure under the Freedom of Information Act.

UNCLASSIFIED

UNCLASSIFIED

APPENDIX B MEMBERS

WORKING GROUP PARTICIPANTS

Organizations participating on the Working Group:

Defense Communications Agency
Defense Intelligence Agency
Department of Commerce (NBS)
Department of Energy
Department of Transportation
Department of Treasury
Director of Central Intelligence
Federal Emergency Management Agency
General Services Administration
Intelligence Community Staff
National Communications Systems
National Security Agency
Office of the Joint Chiefs of Staff
Office of the Secretary of Defense
United States Air Force
United States Army

UNCLASSIFIED

UNCLASSIFIED

APPENDIX C

REFERENCES

1. Campbell, Bruce J. and Carr, Frank J., "Joint Statement before the Subcommittee on Transportation, Aviation, and Materials House Committee on Science and Technology Hearings on Computer and Communications Security and Privacy, U.S. House of Representatives," 24 September 1984.

2. Community Counterintelligence Staff/Intelligence Community Staff, Hostile Intelligence Services Threat and United States Countermeasures, January 1984.

3. Computer Security Technical Consortium, DoD Computer Security Initiative: A Status Report and R&D Plan, March 1981.

4. Defense Science Board Task Force on Computer Security, Edited by Ware, Wills H., Security Controls for Computer Systems, October 1979.

5. Department of Defense Computer Security Center, Automated Information Systems Security (AISS) Survey, 27 April 1984.

6. Department of Defense Computer Security Center, Computer Security Threat, January 1984.

7. Department of Treasury, Directive Manual, 23 November 1983.

8. Federal Emergency Management Agency, FEMA Manual 1540.2 "Automated Information Systems (AIS) Security," September 1984.

9. Federal Personnel Manual, Chapter 731 "Personnel Suitability," 6 January 1984.

10. Federal Personnel Manual, Chapter 732 "Personnel Security," 6 January 1984.

11. Interagency Group/Countermeasures, Countermeasures Macro Resources Data Study, 7 December 1984.

12. Interagency Group/Countermeasures, NSSD-2 Countermeasures Organization Study, July 1983.

13. Kusserow, Richard P., Computer-Related Fraud and Abuse in Government Agencies, July 1983.

14. Kusserow, Richard P., "Statement before Subcommittee on Transportation, Aviation and Materials Committee on Science and Technology," 24 September 1984.

UNCLASSIFIED

UNCLASSIFIED

15. Myers, Philip A., Subversion: The Neglected Aspect of Computer Security, June 1980.

16. National Bureau of Standards. Proceedings of the Fifth Seminar on the DoD Computer Security Initiative, 24-26 May 1982.

17. National Communications Security Committee, The Status of Communications Security in the Federal Government for 1982-1983, 10 February 1983.

18. National Security Telecommunications Advisory Committee, Automated Information Processing Task Force Report, 10 June 1983.

19. National Security Telecommunications Advisory Committee, Automated Information Processing Task Force Interim Report, 15 February 1984.

20. National Security Telecommunications Advisory Committee, Automated Information Processing (AIP) Task Force Final Report, 25 October 1984.

21. Podell, Harold J., Ph.D., Computer Fraud - The Threat and Possible Solutions, 29 November 1984.

22. Policy Survey Committee, Survey of Federal Computer Security Policies, 5 December 1980.

23. R&D Sub-Task Force Report for the SECDEF Initiative, The Scope and Direction of the Computer Security R&D Program, 18 July 1984.

24. Stanford Research Institute, Systems Auditability and Control Study - Data Processing Audit Practices Report.

25. Task Force on Computer Crime Section of Criminal Justice: American Bar Association, Report on Computer Crime, June 1984.

26. United States General Accounting Office, "Better Guidance Would Improve ADP Evaluations in Support of the Federal Managers Financial Integrity Act of 1982," 21 June 1984.

UNCLASSIFIED

UNCLASSIFIED

APPENDIX D

GLOSSARY

Automated Information Systems (AIS): Systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

Automated Information Systems Security (AISS): Protection afforded to automated information systems in order to prevent exploitation, unauthorized access or related technical intelligence threats to classified and sensitive information and to ensure authenticity and accountability. Such protection results from the application of technical, procedural and administrative measures to AISS which contain information, or themselves are of use to an adversary, and may include the physical protection of sensitive technical security information/material.

BLACKER: A system of hardware and software that provides protection of information in a data switched network such as the Defense Digital Network (DDN). This system implements what is known as "end-to-end encryption." It uses a combination of cryptographic and computer security techniques to provide this protection.

Sensitive Information: Unclassified government or government-derived information which requires a degree of protection and which should not be made generally available. The loss of such information could adversely affect the national interest.

Trusted Computer System: Employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

UNCLASSIFIED

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP97M00248R000500170013-4

25X1

[redacted]

[redacted]

25X1

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP97M00248R000500170013-4