NTISSP No. 200
15 July 1987

NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

NATIONAL POLICY

ON

CONTROLLED ACCESS PROTECTION

NTISSC

NATIONAL

TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY
COMMITTEE

OFFICE OF THE CHAIRMAN

FOREWORD

This policy defines a minimum level of protection for automated information systems operated by executive branch, agencies and departments of the Federal Government and their contractors. The private sector is encouraged to apply the precepts of this policy wherever it perceives the need.

Questions pertaining to this policy should be directed to the Executive Secretary, National Telecommunications and Information Systems Security Committee (NTISSC), Fort George G. Meade, MD 2O755-6000.

DONALD C. LATHAM
Chairman

NATIONAL POLICY
ON
CONTROLLED ACCESS PROTECTION

SECTION I - POLICY

1. All automated information systems which are accessed by more than one user, when those users do not have the same authorization to use all of the classified or sensitive unclassified information processed or maintained by the automated information system, shall provide automated Controlled Access Protection for all classified and sensitive unclassified information. This minimum level of protection shall be provided within five years of the promulgation of this policy.

SECTION II – DEFINITION

2. Automated Information Systems are systems which create, prepare, process, or manipulate information in electronic form, and include computers, word processing systems, other electronic information handling systems, and associated equipment. See also Office of Management and Budget Circular A-130, Management of Federal Information Resources.

Controlled Access Protection is the C2 level of protection described in the Trusted Computer System Evaluation Criteria. The major characteristics of Controlled Access Protection are addressed in Section IV.

SECTION III - APPLICABILITY

3. This policy applies to executive branch agencies and departments of the Federal Government and their contractors who process classified or sensitive unclassified information in automated information systems.

SECTION IV - MINIMUM SECURITY REQUIREMENTS

4. A technical description of the security requirements for a minimum level of protection (i.e., Controlled Access Protection) is the C2 level of protection described in the Trusted Computer System Evaluation Criteria. Based upon a system risk assessment, additional protections may be required. Major characteristics of Controlled Access Protection are:

a. Individual accountability through identification and authentication of each individual automated information system user;

b. Maintenance of audit trails of security-relevant events;

c. An, ability to control a user's access to information according to the authorization the user has; and

d. Preventing one user from obtaining another user's residual data.

SECTION V - EXCEPTIONS

5. It is recognized that strengthening the hardware or software security features of an automated information system may be prohibitively costly, technically unsound, or may impact adversely on meeting operational requirements in a timely fashion. Exceptions are appropriate in these circumstances. Such exceptions shall be granted by the approving authority of a department or agency only after a written determination is made citing the adverse impact and alternative remedial actions. Heads of departments or agencies shall ensure continuous progress is made toward reducing or eliminating the circumstances causing the need for the exception.

VI - RESPONSIBILITIES

6. Heads of departments and agencies shall ensure that the provisions of this policy are carried out.

DISTRIBUTION:

NSA
NSC
OMB (Intel Branch NSD)
ODASD (C^3I) (Greg O'Hara) (2)
OJCS (J6) (2)
CSA (DAIM-OI) (2)
CSA (DAMI-CIC) (2)
CSA (DALO-SMC) (2)
CSA (DAMA-CSC) (2)
CNO (OP-94l) (3)
CMC (CC) (5)
USCINCCENT (RCJ6-O) (2)
USCINCEUR (C3S) (2)
USCINCLANT (C35) (2)
USCINCPAC (C3S) (2)
USCINCRED (RCC4S-O) (2)
USCINCSO (J6) (2)
HQ USAF (SITT) (3)
HQ SPACECMD (2)
HQ MAC (SC) (2)
EQ SAC (SC) (2)
EQ TAC (SC) (2)
AFCSC (SRMP) (20)
AFCSC/EPVL
HQ CENTCOM
COMUSFORCARIB (J6) (2)
COMUSFJAPAN (J6) (2)
COMUSFKOREA (J6) (2)
DIR ARFCOS (2)
DCSO (CODE B2l0) (20)
DIA (RSI-5) (10)
DIS (V0410) (5)
DLA (DLA-TI) (2)
DNA (LECD)
DIR TRI-TAC (TT-SC)
CDR JTE/JTC3a
CDR USAINSCOM (IAOPS-OP-P) (15)
CDR USACSI,A (SELCL-NMP) (5)
COMNAVSECGRU (G-61) (15)
COMDT COGARD (G-TTS4) (3)
COMCOGARDLANTAREA
COMCOGARDPACAREA
COMCOGARDONE
COMCOGARDTWO
COMCOGARDTHREE
COMCOGARD FIVE

COMCOGARDSEVEN
COMCOGARDEIGHT
COMCOGARDNINE
C OMCOGARDELEVEN
COMCOGARDTWELVE
COMCOGARDTHIRTEEN
COMCOCARDFOURTEEN
COMCOGARDSEVENTEEN
COMNAVELEXSYSCOM (PDE 110-231) (3)
DCMS (T60) (6)
CG MCDEC (DEVCEN C3) (2)
Dept. of Agriculture (MSD/FAS) (2)
Dept. of Commerce (IS) (2)
Dept. of Energy (CSTM) (2)
Dept. of Health & Human Services (IG) (2)
Dept. of Interior (AMO) (2)
Dept. of Justice (JMD/SS) (2)
Dept. of State (ASC) (4)
Dept. of Transportation (OIS M-50) (2)
Dept. of Treasury (AIT) (10)
CIA (OC-CSD) (2)
CIA (DIR OIT) (2)
CIA (ISSG/OS) (2)
CIA (Chief, TEMPEST Division, OS) (2)
DIR, IC STAFF (IIHC) (2)
DIR, IC STAFF (DCI SECURITY COMMITTEE) (2)
DIR, IC STAFF (POLICY AND PLANNING STAFF) (2)
DCA (Code B310)
DMA OTS (OMD)
DMA IS
Drug Enforcement Administration (AIOC) (2)
FAA (ADL-l5) (6)
FBI (TSD) (5)
FCC (OMD) (2)
FEMA (OP-IR) (7)
GSA (KJS) (6)
NASA (NIS) (20)
NASA (TS) (15)
NCS (MGR) (2)
NRC (572l—NMBB) (2)