

FOIA MARKER

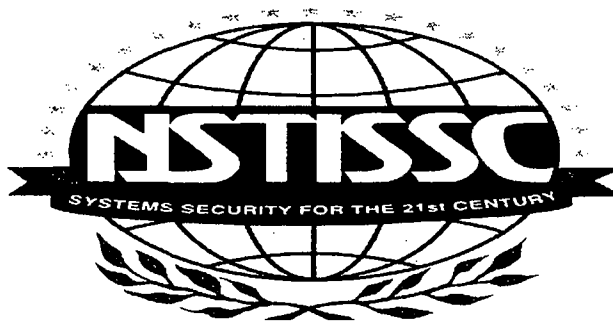
This is not a textual record. This is used as an administrative marker by the William J. Clinton Presidential Library Staff.

Collection/Record Group: Clinton Presidential Records
Subgroup/Office of Origin: Office of Science and Technology
Series/Staff Member:
Subseries:

OA/ID Number: 43311
FolderID:

Folder Title:
National Security Telecommunication and Information Systems Security Committee (NSTISSC)

Stack:	Row:	Section:	Shelf:	Position:
S	1	1	7	3



FACT SHEET

NSTISSP No. 11

National Information Assurance Acquisition Policy

January 2000

Background

(1) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products is issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

(2) The NSTISSC was established by National Security Directive (NSD) No. 42, dated July 1990, and is responsible for developing and promulgating national policies applicable to the security of national security telecommunications and information systems.

Introduction

(3) The technological advances and threats of the past decade have drastically changed the ways we think about protecting our communications and communications systems. Three factors are of particular significance:

- The need for protection encompasses more than just confidentiality;
- Commercial off-the-shelf (COTS) security and security-enabled information assurance (IA) products are readily available as alternatives to traditional NSA-developed and produced communications security equipment (i.e., government-off-the shelf (GOTS) products); and
- An increased and continuing recognition that the need for IA transcends more than just the traditional national security applications of the past.

(4) In the context of the second of the above factors, it is important that COTS products acquired by U.S. Government Departments and Agencies be subject to a standardized evaluation process which will provide some assurances that these products perform as advertised. Accordingly, the attached policy has been developed as a means of addressing this problem for those products acquired for national security applications. The policy also rightfully points out that protection of systems encompasses more than just acquiring the right product. Once acquired, these products must be integrated properly and subject to an accreditation process which will ensure total integrity of the information and systems to be protected.

Policy

(5) Information Assurance (IA) shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated Government Off-the-Shelf (GOTS) or Commercial Off-the-Shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products should provide for the *availability* of the systems; ensure the *integrity* and *confidentiality* of information, and the *authentication* and *non-repudiation* of parties in electronic transactions.

(6) Effective 1 January 2001, preference shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which have been evaluated and validated, as appropriate, in accordance with:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;
- The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or
- The NIST Federal Information Processing Standard (FIPS) validation program.

(7) The evaluation/validation of COTS IA and IA-enabled IT products will be conducted by accredited commercial laboratories, or the NIST.

(8) By 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified in paragraph (6), above, shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in the three sub-bullets.

(9) The acquisition of all GOTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information shall be limited to products which have been evaluated by the NSA, or in accordance with NSA-approved processes.

(10) Normally, a complementary combination of IA/IA-enabled products is needed to provide a complete security solution to a given environment. Thus, in addition to employing evaluated and validated IA/IA-enabled products, a solution security analysis should be conducted as part of the certification and accreditation process. In support of this, NSA shall provide guidance regarding the appropriate combinations and implementation of GOTS and COTS IA and IA-enabled products.

(11) Subject to policy and guidance for non-national security systems, departments and agencies may wish to consider the acquisition and appropriate implementation of evaluated and validated COTS IA and IA-enabled IT products. The use of these products may be appropriate for systems which process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems which may be associated with the operation and/or maintenance of critical infrastructures as defined in Presidential Decision Directive No. 63 (PDD-63), Critical Infrastructure Protection.

Responsibilities

(12) Heads of U.S. Departments and Agencies are responsible for ensuring compliance with the requirements of this policy.

Exemptions and Waivers

(13) COTS or GOTS IA and IA-enabled IT products acquired prior to the effective dates prescribed herein shall be exempt from the requirements of this policy. Information systems in which those products are integrated should be operated with care and discretion and evaluated/validated IA products and solutions considered as replacement upgrades at the earliest opportunity.

(14) Waivers to this policy may be granted by the NSTISSC on a case-by-case basis. Requests for waivers, including a justification and explanatory details, shall be forwarded through the Director, National Security Agency (DIRNSA), ATTN: V1, who shall provide appropriate recommendations for NSTISSC consideration. Where time and circumstances may not allow for the full review and approval of the NSTISSC membership, the Chairman of the NSTISSC is authorized to approve waivers to this policy which may be necessary to support U.S. Government operations which are time-sensitive, or where U.S. lives may be at risk.



FACT SHEET

NSTISSP No. 11

National Information Assurance Acquisition Policy

January 2000

Background

(1) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products is issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

(2) The NSTISSC was established by National Security Directive (NSD) No. 42, dated July 1990, and is responsible for developing and promulgating national policies applicable to the security of national security telecommunications and information systems.

Introduction

(3) The technological advances and threats of the past decade have drastically changed the ways we think about protecting our communications and communications systems. Three factors are of particular significance:

- The need for protection encompasses more than just confidentiality;
- Commercial off-the-shelf (COTS) security and security-enabled information assurance (IA) products are readily available as alternatives to traditional NSA-developed and produced communications security equipment (i.e., government-off-the shelf (GOTS) products); and
- An increased and continuing recognition that the need for IA transcends more than just the traditional national security applications of the past.

(4) In the context of the second of the above factors, it is important that COTS products acquired by U.S. Government Departments and Agencies be subject to a standardized evaluation process which will provide some assurances that these products perform as advertised. Accordingly, the attached policy has been developed as a means of addressing this problem for those products acquired for national security applications. The policy also rightfully points out that protection of systems encompasses more than just acquiring the right product. Once acquired, these products must be integrated properly and subject to an accreditation process which will ensure total integrity of the information and systems to be protected.

Policy

(5) Information Assurance (IA) shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated Government Off-the-Shelf (GOTS) or Commercial Off-the-Shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products should provide for the *availability* of the systems; ensure the *integrity* and *confidentiality* of information, and the *authentication* and *non-repudiation* of parties in electronic transactions.

(6) Effective 1 January 2001, preference shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which have been evaluated and validated, as appropriate, in accordance with:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;
- The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or
- The NIST Federal Information Processing Standard (FIPS) validation program.

(7) The evaluation/validation of COTS IA and IA-enabled IT products will be conducted by accredited commercial laboratories, or the NIST.

(8) By 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified in paragraph (6), above, shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in the three sub-bullets.

(9) The acquisition of all GOTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information shall be limited to products which have been evaluated by the NSA, or in accordance with NSA-approved processes.

(10) Normally, a complementary combination of IA/IA-enabled products is needed to provide a complete security solution to a given environment. Thus, in addition to employing evaluated and validated IA/IA-enabled products, a solution security analysis should be conducted as part of the certification and accreditation process. In support of this, NSA shall provide guidance regarding the appropriate combinations and implementation of GOTS and COTS IA and IA-enabled products.

(11) Subject to policy and guidance for non-national security systems, departments and agencies may wish to consider the acquisition and appropriate implementation of evaluated and validated COTS IA and IA-enabled IT products. The use of these products may be appropriate for systems which process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems which may be associated with the operation and/or maintenance of critical infrastructures as defined in Presidential Decision Directive No. 63 (PDD-63), Critical Infrastructure Protection.

Responsibilities

(12) Heads of U.S. Departments and Agencies are responsible for ensuring compliance with the requirements of this policy.

Exemptions and Waivers

(13) COTS or GOTS IA and IA-enabled IT products acquired prior to the effective dates prescribed herein shall be exempt from the requirements of this policy. Information systems in which those products are integrated should be operated with care and discretion and evaluated/validated IA products and solutions considered as replacement upgrades at the earliest opportunity.

(14) Waivers to this policy may be granted by the NSTISSC on a case-by-case basis. Requests for waivers, including a justification and explanatory details, shall be forwarded through the Director, National Security Agency (DIRNSA), ATTN: V1, who shall provide appropriate recommendations for NSTISSC consideration. Where time and circumstances may not allow for the full review and approval of the NSTISSC membership, the Chairman of the NSTISSC is authorized to approve waivers to this policy which may be necessary to support U.S. Government operations which are time-sensitive, or where U.S. lives may be at risk.

National Security Telecommunications

and
NSTISSC

Information Systems Security Committee



WHAT'S IN A NAME?

(WE'VE HAD A FEW!)

1953

United States COMSEC Board (USCSB)

1979

National COMSEC Committee (NCSC)

1984

**National Telecommunications and Information Systems
Security Committee (NTISSC)**

1990

National Security Telecommunications and Information

MILESTONES IN OUR HISTORY

- **PRESIDENTIAL DIRECTIVE, OCTOBER 1952**

- COMSEC: a national responsibility
- SECDEF = Executive Agent

- **NSDD-145, SEPTEMBER 1984**

- Computer security: a national responsibility
- Telecommunications and AIS security become DoD responsibility
- DIRNSA = National Manager

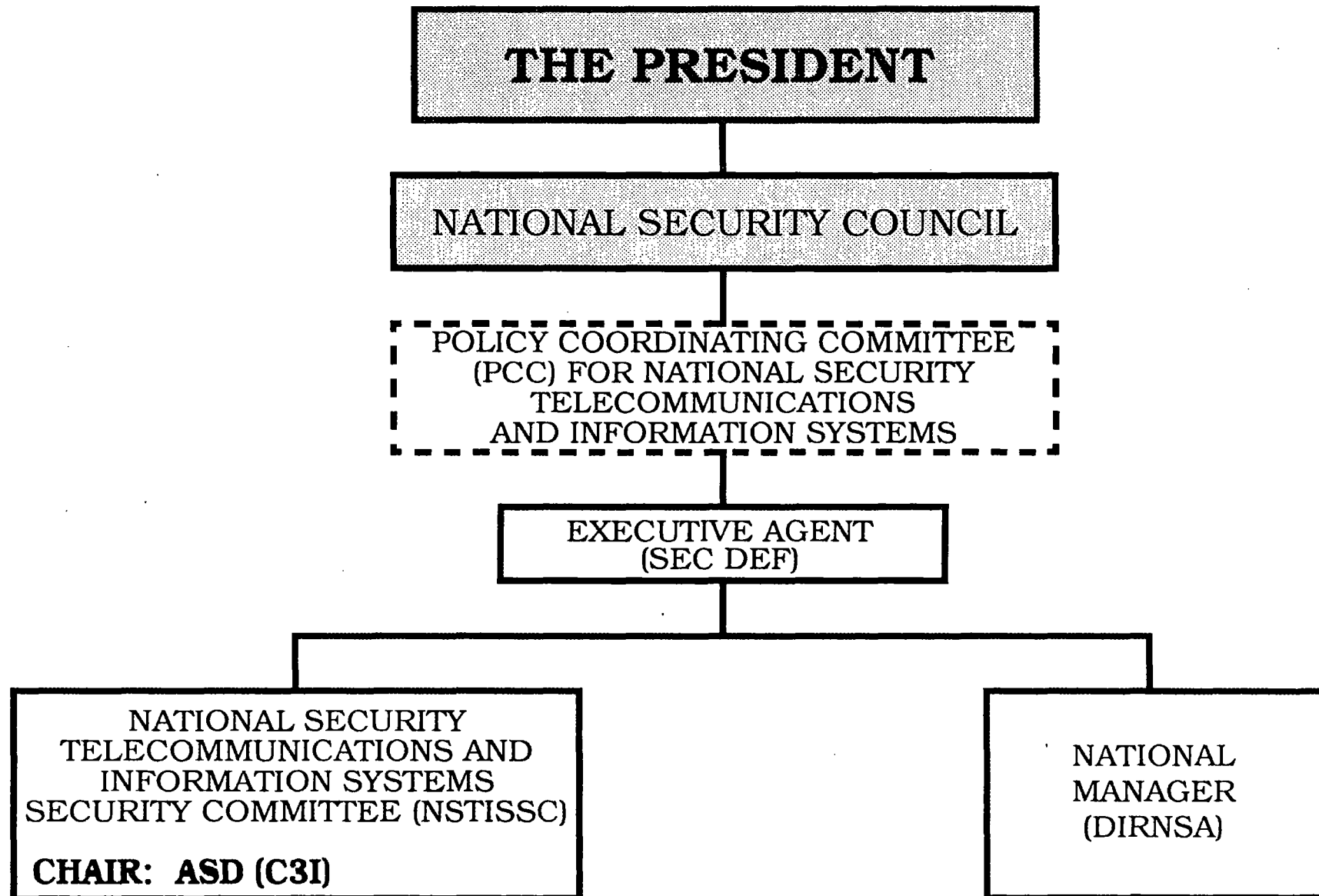
- **P.L. 100-235, COMPUTER SECURITY ACT, JANUARY 1988**

- Governmentwide computer security: national priority
- NIST = most unclassified; NSA = other + technical advice
- NIST: develop standards and guidelines with NSA's assistance

- **NSD-42, JULY 1990**

- complied with P.L. 100-235

NSD-42 STRUCTURE



STS/SISS MEMBERS

- **21 Members**
- **20 Observers**

**Overall 60 Departments and Agencies Represented on
Committee, Subcommittees and Working Groups.**

NSTISSC

National Security Telecommunications
and Information Systems Security Committee

Chair: Mr. Arthur L. Money
Senior Civilian Official for the OASD (C³I)

SISS

Subcommittee on
Information Systems Security

Chair: Mr. John Davis, NCSC

STS

Subcommittee on
Telecommunications Security

Chair: Mr. Thomas Burke, GSA

ACTIVE JOINT WORKING

Annual
Assessment

Key
Management
Infrastructure

Glossary

TEMPEST
Advisory
Group

NSTISSC ISSUE GROUPS

Information Assurance

Champions:

Mr. Thomas Burke, GSA
Mr. Richard R. Schaeffer, Defense
Ms. Judith Cuddehe, Commerce

Information
Infra-
structure

Inter-
operability

C & A

Improve INFOSEC Guidance & Services

Champions:

Mr. Michael J. Jacobs, NSA
VACANT

Marketing

Re-
engineering

Policy/
Oversight

Education, Training & Awareness

Champions:

VACANT
VACANT

EKMS
Training

Policy/
Guidelines

INFOSEC
Trng Tools

May 1998

WHAT WE DO...

- * Develops policies, guidelines, instructions, standards**
- * Systems security guidance**
- * Annual assessment of "health" of national security systems**
- * Release approval to foreign governments and international organizations**
- * Maintain national issuance system**

NSTISSC OFFSITE

13 - 16 APRIL 1998

**Theme: Building Stronger Partnerships --
 A Team Approach to Information Security**

175 Participants From:

Government

Industry

Academia

NSTISSC OFFSITE

13 - 16 APRIL 1998

Electronic Commerce

Smart Cards

Legal and Ethical Issues

Year 2000

PDD on Critical Infrastructure Protection

Fed CIRC

Also, ...

Break-Out Sessions

Demos

Reengineering Training

EXECUTIVE SESSION

Tuesday, 14 April 1998

Chair: Mr. Arthur L. Money

Discussion Issues:

- * A national policy for information assurance**

Leader: Thomas R. Burke, GSA

- * Implementation of NSTISSP 5 and NSTISSD 503:**

Incident response and vulnerability reporting for national security systems

Leader: Michael J. Jacobs, NSA

EXECUTIVE SESSION

Tuesday, 14 April 1998

Other Issues:

- * Draft Policy on Destruction of Magnetic Media**
- * Certification and Accreditation**
- * PKI**
- * Insider Threat**
- * Interoperability**
- * Annual Assessment**
- * INFOSEC Professionalization**

NSTISSC MEMBERS

- **CHAIR: ASD (C3I)**

State
Treasury
Attorney General
Commerce
Transportation
Energy
OMB
NSC
DCI
FBI
FEMA
GSA

Defense
JCS
Army
Navy
Air Force
Marines
NSA
NCS
DIA

- **NSTISSC Observers**

Education
FCC
NASA
NIST
NRC

DISA
NIMA
SISS
SPB

SPB ACTIONS REQUIRED

Policy Integration Committee (PIC):

- * Develop policy for protection of SBU that relates to infrastructure vulnerabilities and technology transfer issue**
- * “Pursue” National AIS policy**

“... in coordination with NSTISSC”

