

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 Agency (NSA) Info

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

Recent CSTB Reports

*LC21: A Digital Strategy for the Library of Congress
Summary of a Workshop on Information Technology
Research for Federal Statistics
Making IT Better: Expanding the Scope of Information
Technology Research to Meet Society's Needs
Networking Health: Prescriptions for the Internet
Summary of a Workshop on Information Technology
Research for Crisis Management
The Digital Dilemma: Intellectual Property in the
Information Age
Being Fluent with Information Technology
Realizing the Potential of C4I: Fundamental Challenges
Funding a Revolution: Government Support for
Computing Research
Trust in Cyberspace
Fostering Research on the Economic and Social
Impacts of Information Technology
Computing and the Humanities: Summary of a
Roundtable Meeting
The Unpredictable Certainty: White Papers
The Evolution of Untethered Communications
More Than Screen Deep: Toward Every-Citizen
Interfaces to the Nation's Information
Infrastructure
Defining a Decade: Envisioning CSTB's Second 10
Years
For the Record: Protecting Electronic Health
Information
Modeling and Simulation: Linking Entertainment
and Defense
Ada and Beyond: Software Policies for the
Department of Defense
Cryptography's Role in Securing the Information
Society
Computing and Communications in the Extreme*

Copies of all CSTB reports are available from:

National Academy Press
2101 Constitution Avenue, NW
Box 285
Washington, D.C. 20055
800-624-6242 toll-free
(or 202-334-3313 in the Washington Metropolitan Area)

Reports can also be viewed and ordered
online at <http://www.nap.edu>

CSTB Membership

DAVID D. CLARK (Chairman), Massachusetts
Institute of Technology
JAMES CHIDDIX, Time Warner Cable
JOHN M. CIOFFI, Stanford University
ELAINE COHEN, University of Utah
W. BRUCE CROFT, University of Massachusetts,
Amherst
SUSAN L. GRAHAM, University of California at
Berkeley
JUDITH HEMPEL, UCSF-Molecular Design Institute
JEFFREY M. JAFFE, Lucent Technologies
ANNA KARLIN, University of Washington
MICHAEL KATZ, University of California at Berkeley
BUTLER W. LAMPSON, Microsoft Corporation
EDWARD D. LAZOWSKA, University of Washington
DAVID LIDDLE, U.S. Venture Partners
TOM M. MITCHELL, WhizBang! Labs, Inc.
DONALD NORMAN, UNext.com
HENRY (HANK) PERRITT, Illinois Institute of
Technology
DAVID A. PATTERSON, University of
California at Berkeley
CHARLES SIMONYI, Microsoft Corporation
BURTON SMITH, Cray Inc.
TERRY SMITH, University of California at Santa
Barbara
LEE S. SPROULL, New York University

Staff:

Marjory S. Blumenthal, Executive Director
Herbert S. Lin, Senior Scientist
Jerry R. Sheehan, Senior Program Officer
Alan S. Inouye, Program Officer
Jon Eisenberg, Program Officer
Gail Pritchard, Program Officer
Elizabeth Grossman, Program Officer
Lynette I. Millett, Program Officer
Janet Briscoe, Office Manager
David (D.C.) Drake, Project Assistant
Margaret Marsh, Project Assistant
Daniel Llata, Sr. Project Assistant
Suzanne Ossa, Sr. Project Assistant
Brandye Williams, Office Assistant

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

NATIONAL RESEARCH COUNCIL
2101 CONSTITUTION AVE., NW
WASHINGTON, D.C. 20418
202-334-2605 (-2318 FAX)

<http://www.cstb.org>

The National Academies

July 2000

What is CSTB?

The Computer Science and Telecommunications Board (CSTB) was established in 1986 to provide independent advice to the federal government on technical and public policy issues relating to computing and communications. Composed of leaders from industry and academia, CSTB conducts studies of critical national issues and makes recommendations to government, industry, and academic researchers. CSTB also provides a neutral meeting ground for consideration of complex issues where resolution and action may be premature. It convenes invitational discussions that bring together principals from the public and private sectors, assuring consideration of all perspectives. The majority of CSTB's work is requested by federal agencies and Congress, consistent with its National Academies context.

A pioneer in framing and analyzing Internet policy issues, CSTB is unique in its comprehensive scope and effective, interdisciplinary appraisal of technical, economic, social, and policy issues. Its mission is to:

Monitor and promote the health of the fields of computer science and telecommunications, with attention to issues of human resources, information infrastructure, and societal impacts generally.

Initiate studies involving computer science and technology and telecommunications as critical resources.

Respond to requests from the government, non-profit organizations, and private industry for advice on computer and telecommunications issues and from the government for advice on computer and telecommunications systems planning, utilization, and modernization.

Foster interaction among the disciplines underlying computing and telecommunications technologies and other fields, in the National Research Council (NRC) and at large.

How Does CSTB Work?

CSTB draws on some of the best minds in the country, inviting experts to participate in its projects as a public service. Studies are conducted by balanced committees without direct financial interests in the topics they are addressing. Those committees meet, confer electronically, and build analyses through their deliberations. Additional expertise from around the country is tapped in a rigorous process of review and critique, further enhancing the quality of CSTB reports. By engaging groups of principals, CSTB gets the facts and insights critical to assessing key issues.

CSTB itself oversees the projects under its aegis. It draws on its members' knowledge of major trends and issues facing the computing and communications industries, the academic research community, and related professions and organizations to identify areas where it can have an impact. The Board meets three times a year to evaluate ongoing studies and consider project options and hot issues.

CSTB Sponsors

CSTB gratefully acknowledges the core support of its public and private sponsors: AFOSR, AT&T, Cisco Systems, DARPA, DOE, Hewlett-Packard, Intel Corporation, Microsoft Research, NASA, NIST, NLM, NSF, ONR, and Sun Microsystems. It appreciates additional project support from DARPA, DOD, GAAC, HP, Interval Corporation, MCI Worldcom, NIH-DHHS, NLM, NSF, Rockefeller Foundation, Sun Microsystems, Texas Instruments, Time Warner Cable, and US West.

The majority of CSTB's funding comes from federal organizations; its private support enables a more diverse portfolio, broader dissemination, and more quality assurance. CSTB's work is performed independently: its sponsors enable but do not influence its work.

CSTB's Current Activities

- The Internet in the Evolving Info Infrastructure
- Global Networks and Local Values
- Computing and Communications Research to Support Info Technology in Government
- Workforce Needs in Information Technology
- Broadband Last Mile Technology
- Embedded Computing Systems
- Fundamentals of Computer Science—Challenges and Opportunities
- Information Technology and Creativity
- Limiting Kid's Access to Porn on the Internet
- Computing Frontiers: Prospects from Biology
- Cyber-security and the Insider Threat to Classified Information
- Collaboration between Mathematical Sciences and Computer Sciences
- Exploring Information Technology Issues for the Behavioral and Social Science

CSTB's Activities Under Development

- Domain Name Systems and Trademarks
- Critical Infrastructure/Information Assurance
- Ultra-Wideband Technologies
- Archiving Digital Materials
- Internet Governance and Sovereignty
- The Internet and Economic Development
- Issues in Software Development
- Digital Democracy
- Information Technology in Education
- Preserving Privacy in the Information Age
- Authentication Technologies and Their Privacy Implications
- Access and Equity: Info Tech for All?
- Living with Information Technology
- Digital Earth
- Software and E-Commerce Patents
- Intellectual Property & Univ.-Industry Relations



Information Assurance

*Protect and Defend
Critical Information Infrastructures
from Cyber-Attack*

*A Balanced Mix of
COTS and GOTS IA Technology*

Louis Giles
lfgiles@missi.ncsc.mil

INFORMATION ASSURANCE

Availability, Integrity, Authentication, Confidentiality, Non-Repudiation
Requiring A Spectrum of Actions

PROTECT

DETECT & REPORT

RESPOND

Enabled by a Holistic, Defense-in-Depth Strategy

Policy & Legal Framework

Protect

Detect & Report

Respond

Information Assurance Solutions

The IA Technology Spectrum

Security-Enabled Technology

Messaging
Web
E-Commerce
Security Protocols

**Mostly
COTS**

Security Technology

Crypto-modules
Network Encryptors
Firewalls / Guards
Malicious Code Detection
Audit Tools

Mix of GOTS and COTS

Security-Relevant Technology

Operating Systems
Network Protocols
Network Components
Network Management Tools
Servers / Hosts

All COTS

COTS - Commercial Off-the-Shelf
GOTS - Government Off-the-Shelf

Information Assurance Solutions Process

Comprised of:

- A Common Security Language
- An IA Framework
- IA Development, Evaluation and Validation
- IA Solution Composition, Testing & Sustainment

A Common Security Language

- Functional requirements
- Assurance requirements -- 7 Evaluated Assurance Levels (EAL)
- Protection Profiles (PP) - User - “I Want”
- Security Targets (ST) - Vendor - “I Will Provide”

- International Mutual Recognition Arrangement
- ISO Standard 15408 Jun 99



US



Canada



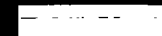
UK



Germany

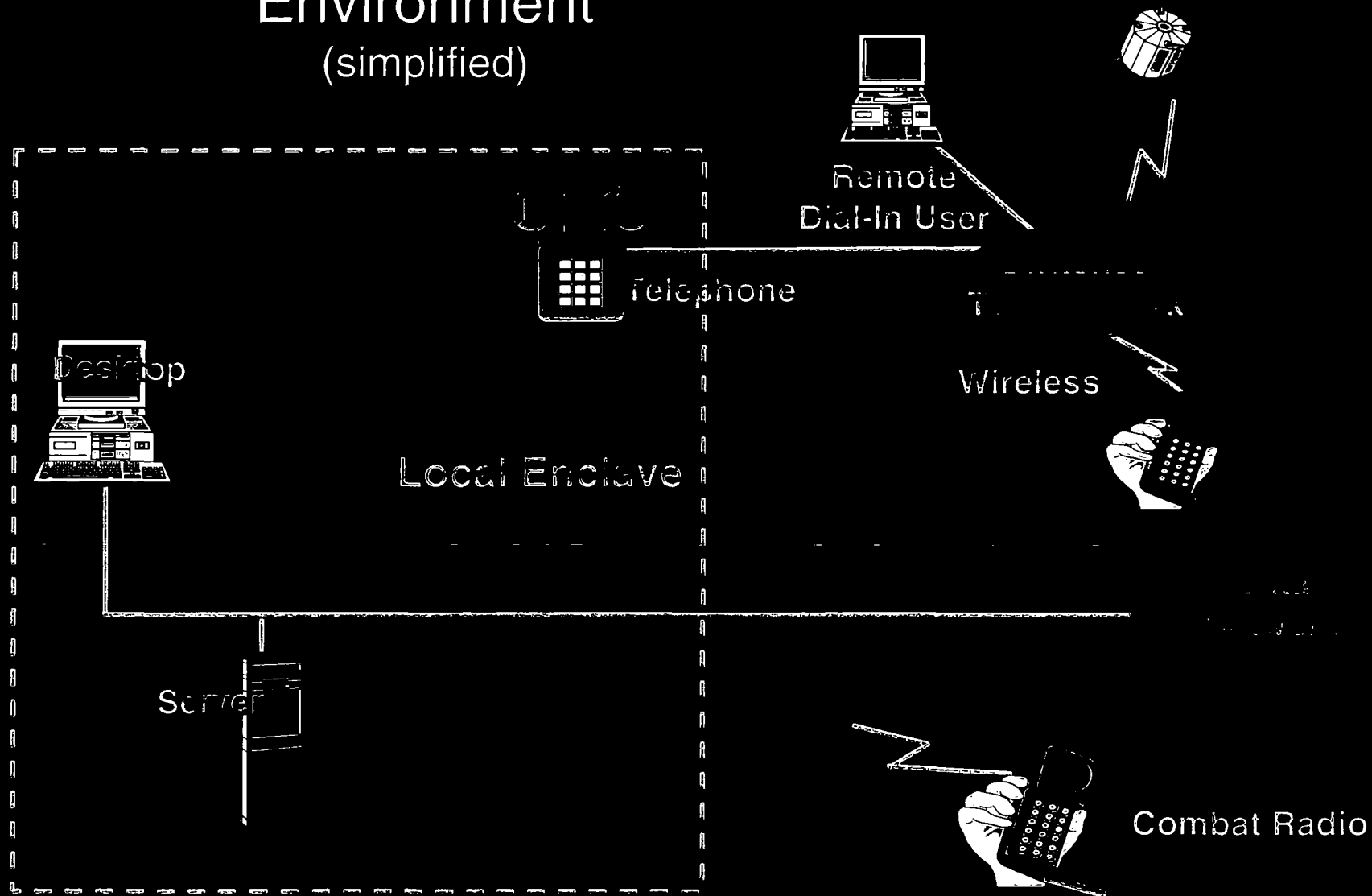


France



Netherlands

Typical Enterprise Cyber Environment (simplified)



Defense In Depth Technology Dimension

Successful Mission Execution

Information Assurance

Personnel

Technology

Operations

Defense In Depth Strategy

Protect &
Defend the
Networks &
Infrastructure

Protect &
Defend the
Enclave
Boundary

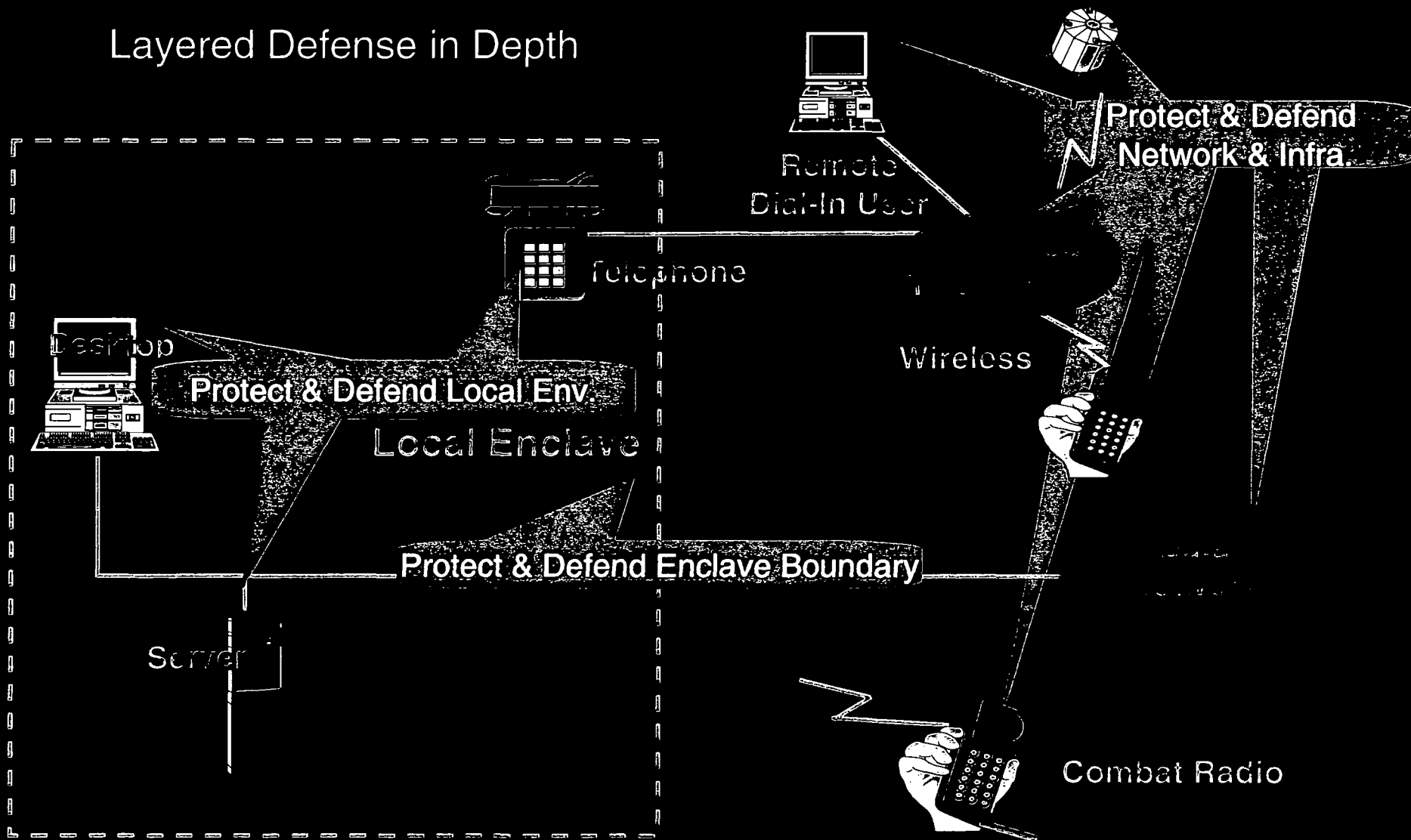
Protect &
Defend the
Computing
Environment

Key
Management /
Public Key
Infrastructure

Overlapping Layers of Protection

IA Solution Framework

Layered Defense in Depth



NSA IA GOTS Development Examples

- **Network Encryption**
 - Fastlane & TacLane ATM, KG 189 SONET
- **Satellite & Ground Station Security**
 - KG 207, Photoplay, KG 247, ACTS
- **E-Mail Guards**
 - SCC SNS, Wang DMS High Assurance Guard (HAG)
- **Secure Wired & Wireless**
 - STE, Digital Cellular, Mobile Satellite
- **Security Tokens/Modules**
 - Fortezza, Fortezza Server Card, Smart Cards, Cornfield
- **Secure Applications**
 - Remote Dial-in Access Solution (RASP)
- **Intrusion Detection Tools**
- **Key Management Infra (KMI) / Public Key Infra (PKI)**
 - EKMS Phase 4, LMD/KP Rel 4, DTD 2000, CAW

NIAP Evaluation Activity

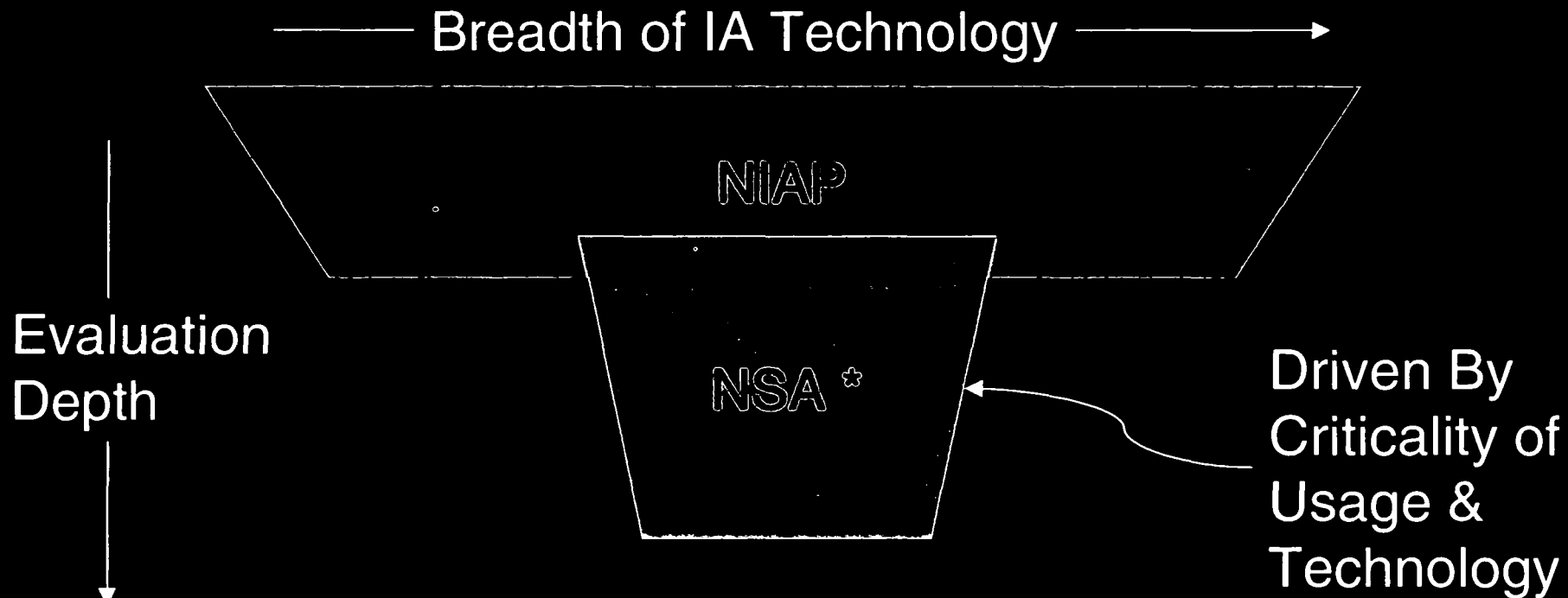
Proprietary

- NSA Trust Technology Assessment Program (TTAP)
 - 7 Commercial Labs (Transitional toward NIAP)
 - » CSC SAIC BAH ARCA Cygnacom
 - COACT National Software Testing Labs
 - Evaluated Products:
 - » CISCO PIX Firewall Lucent Firewall Checkpoint Firewall
 - Voltaire 2 in 1 PC Windows NT4.0 IBM RS6000
 - ITT Dragonfly Guard & Companion
 - Products in Evaluation:
 - » Microsoft SQL Server Sybase DBMS Sun EFS 3.0 Firewall
 - Lucent Firewall Network Associates Gauntlet Firewall
 - Argus PitBull O/S
 - » An Additional 6 Products Under Vendor / Lab Negotiation

National Policy on Acquisition of
Information Assurance (IA) Products
NSTISSP No. 11

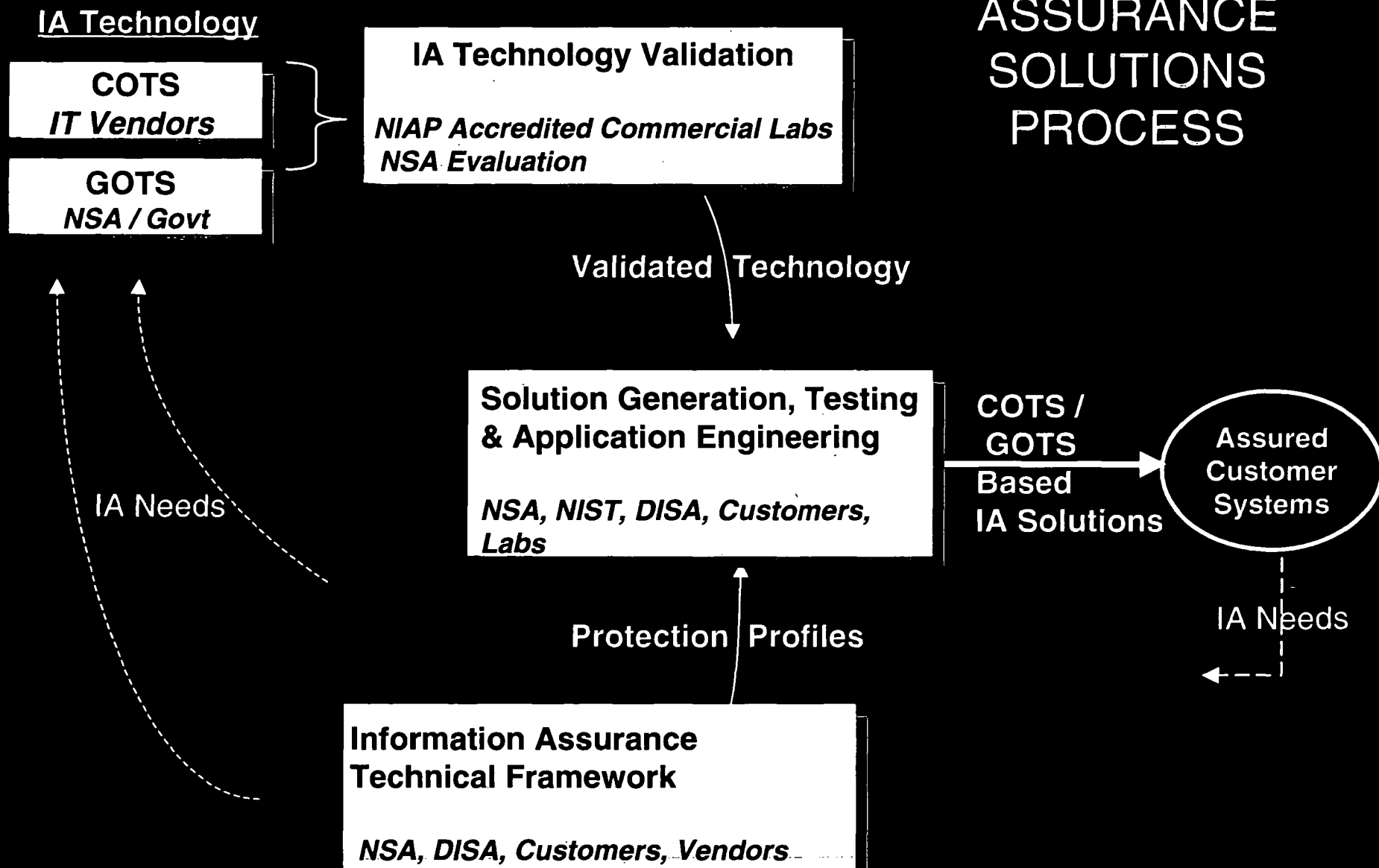
- Evaluated IA Products Preferred - Jan 01
- Evaluated Products Required - Jul 02
- Solution Security Analysis Required
(As a Part of Certification & Accreditation)

Evaluation & Validation Augmentation



- * For COTS, NSA Deep Eval Only In Conjunction with NIAP Eval
- * EAL 5, 6, 7 Test and Vulnerability Assessment

INFORMATION ASSURANCE SOLUTIONS PROCESS



COTS - Commercial Off-the-Shelf
GOTS - Government Off-the-Shelf

NIAP = NIST / NSA National Information Assurance Partnership

16-Mar-00

FOR OFFICIAL USE ONLY

13

INFORMATION ASSURANCE PARTNERSHIP

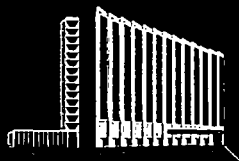


Government

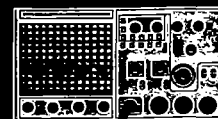
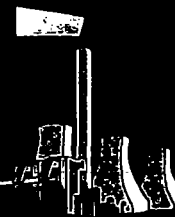
NIST

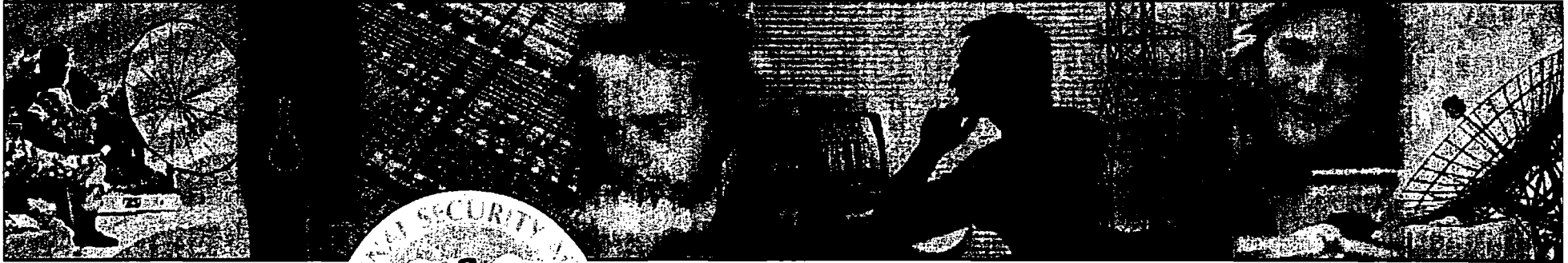


IT Vendors



Users



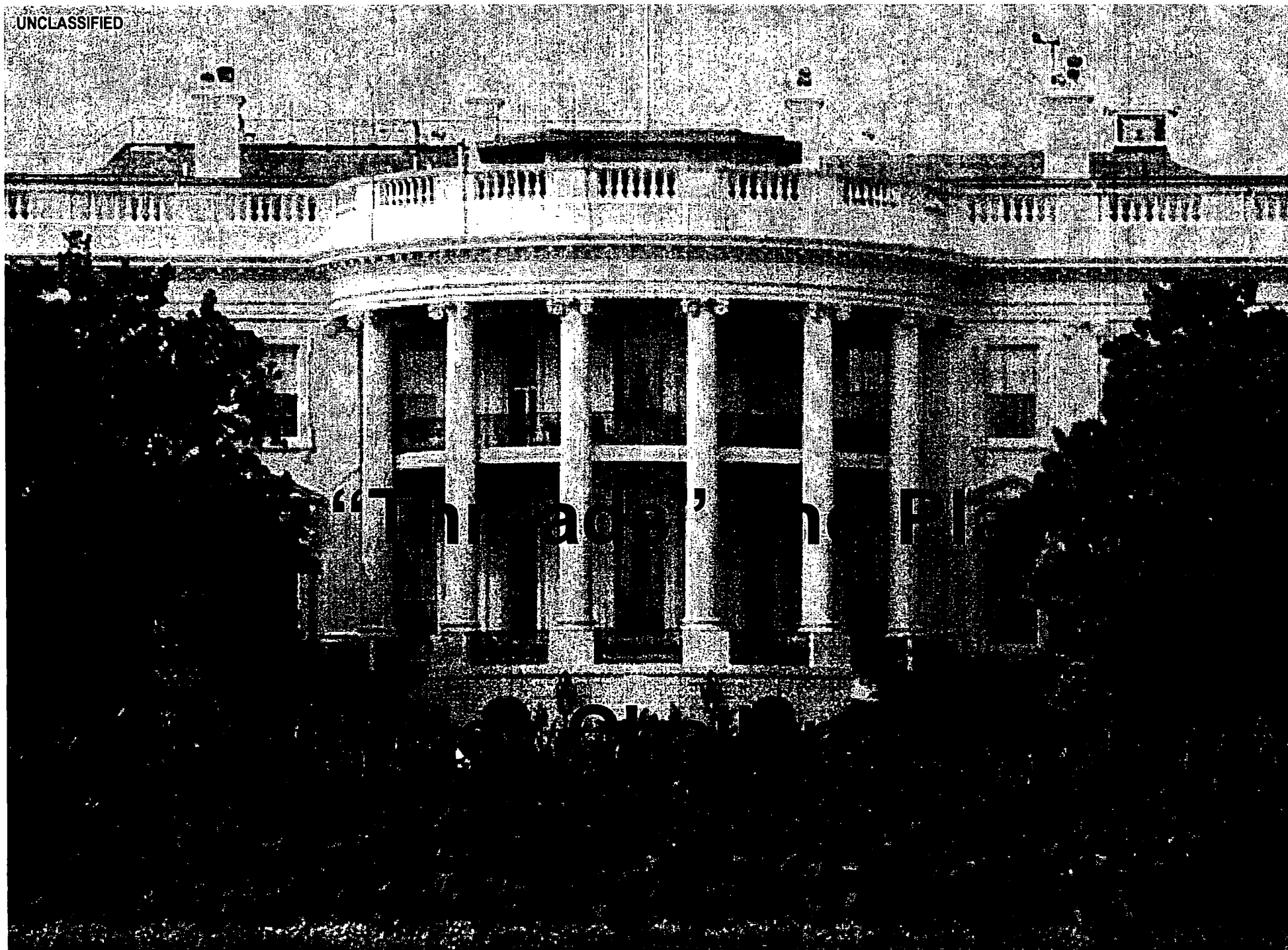


The Policy Challenge

Daniel J. Knauf

Chief, ISSO Policy and Corporate Support (I4)

UNCLASSIFIED



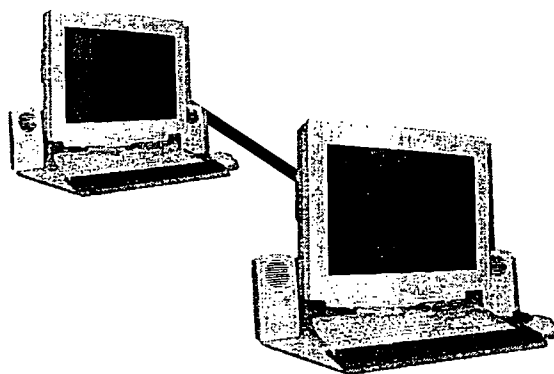
U.S. Information Protection

Past



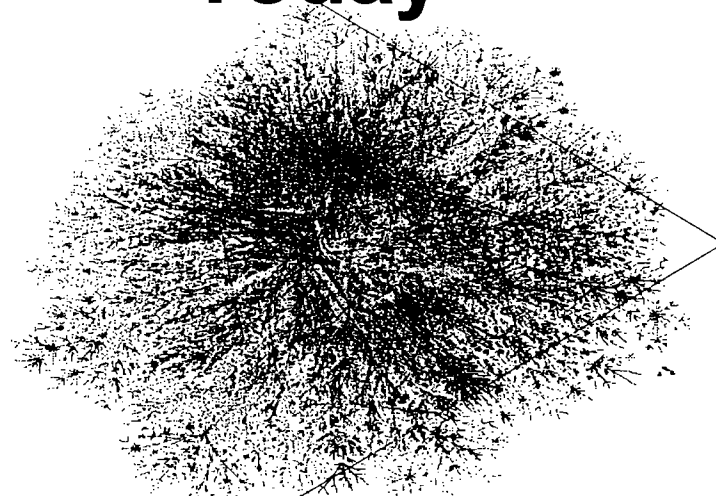
COMSEC

Yesterday



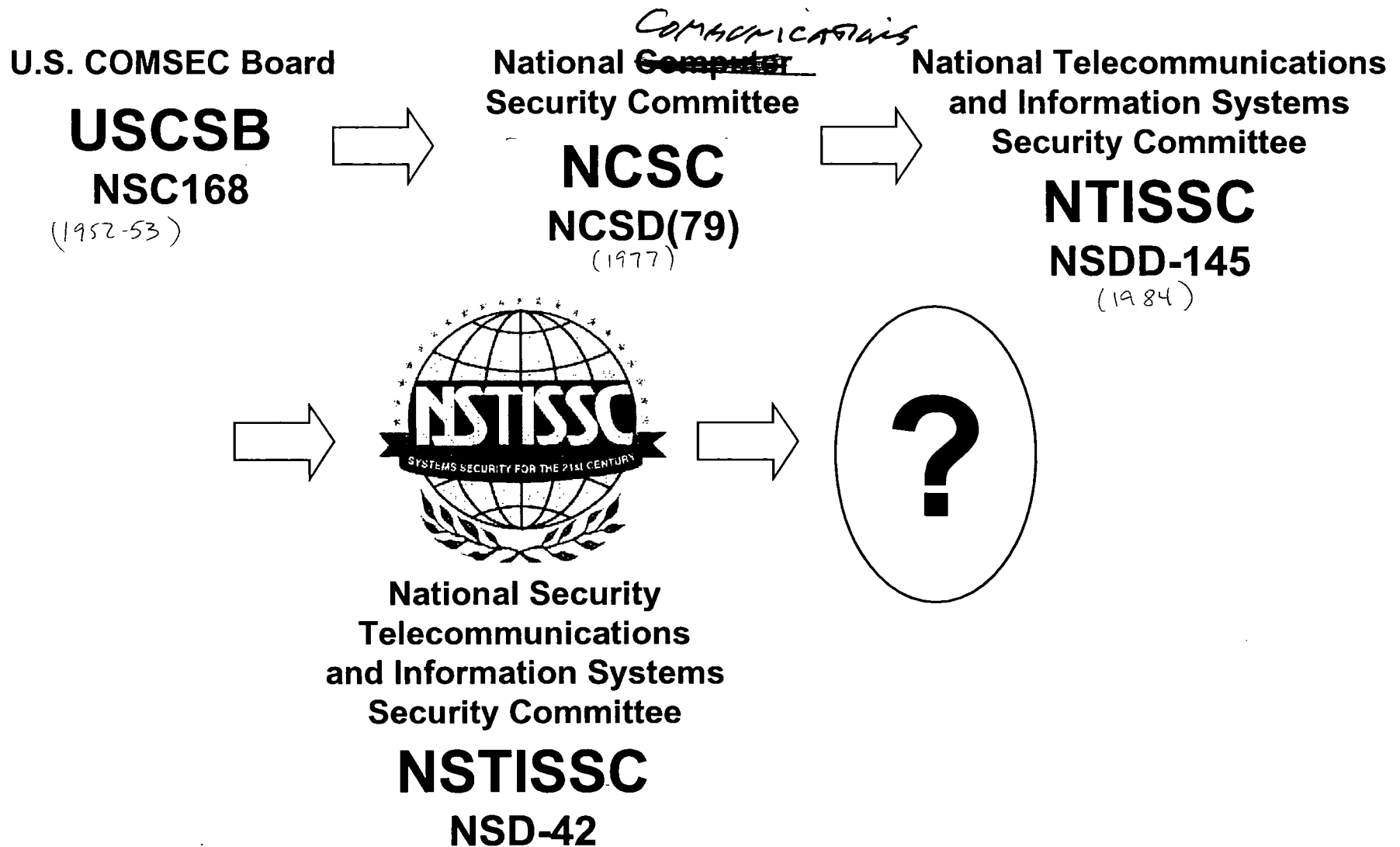
INFOSEC

Today



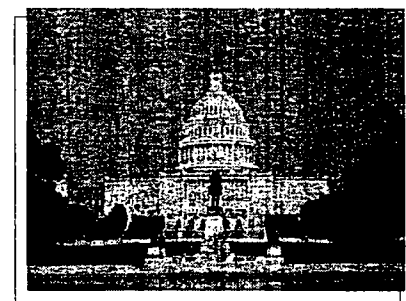
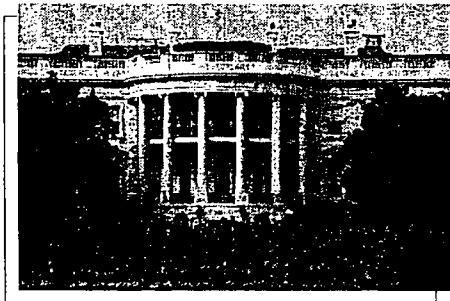
Information Assurance

Evolution of Policy Structures



INFOSEC Authorities

- ◆ **E.O. 12333 (Dec 81)**
 - **United States Intelligence Activities**
- ◆ **NSD-42 (Jul 90)**
 - **National Policy for the Security of National Security Telecommunications and Information Systems**
- ◆ **DoD Directive 5200.5 (Apr 90)**
- ◆ **DoD Directive 5200.28 (Mar 88)**
- ◆ **Computer Security Act of 1987 (PL 100-235)**



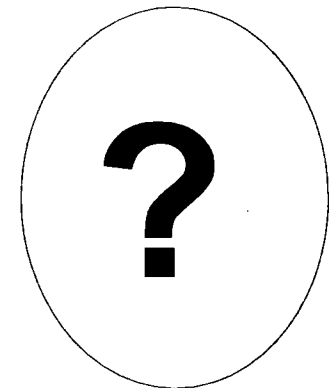
Joint Security Commission

Presidential Decision Directive (PDD) 29

Security Policy Board (ISSC?)

Joint Security Commission II

Security Policy Board/EXCOM



Oklahoma City

PDDs

Commission on

?

- ◆ National Coordinator and Critical Infrastructure Coordinating Group (CICG)
- ◆ Critical Infrastructure Assurance Office (CIAO)
- ◆ National Infrastructure Protection Center (NIPC)
- ◆ Lead Agencies (Sectors and Special Functions)
- ◆ Sector Liaison Officers, Sector Coordinators, and Functional Coordinators