

IT/02-0855

NIST Presentation on the Status  
of ISO/IEC 17799 —  
Management of IT Security

Alicia Clay, Ph.D.

National Institute of Standards and Technology

Computer Security Division

# Outline

- ¥ What 17799 is and what it isn't
- ¥ International visions for use
- ¥ Interest in Part 2
- ¥ Implications for US industries
- ¥ How to get involved

# What 17799 Is and What It Isn't

*give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is **intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.***

- ¥ A starting point for developing organization specific guidance
- ¥ Addresses topics in terms of policies and general good practices.

# What 17799 Is and What It Isn't

High-level overview of the basic issues involved in each of the following topic areas

- ☞ Organizational security policy
- ☞ Organizational security infrastructure
- ☞ Asset classification and control
- ☞ Personnel security
- ☞ Physical and environmental security
- ☞ Communications and operations management
- ☞ Access control
- ☞ Systems development and maintenance
- ☞ Business continuity management
- ☞ Compliance

*Not all of the guidance and controls may be applicable; additional controls may be required*

# What 17799 Is and What It Isn't

- ∕ Does not provide definitive or specific material on any security topic.
- ∕ °Does not provide enough information to support an in-depth organizational information security review.
- ∕ Does not provide the detailed conformance specifications for an organizational information security management program (which would be needed for a certification program such as exists with ISO 9000).

# International Visions For Use

Editors note on the use of 17799

*use of the word should is appropriate for this document. Any more mandatory directions can be based on the standard but should not be part of this document nor be part of the revision process.*

11 of the 14 countries responding to the Editors survey stated that it should not include a certification scheme

6 of the 14 stated that it would be useful to be able to measure or otherwise indicate compliance to the standard

# 17799 Part 2?

*more mandatory directions based on the standard*

*A measure of compliance*

∕Quality information security management? (ala ISO 9000)

∕Common criteria for information security management?

∕*Part of larger certification and accreditation scheme(s)*

# Implications for US Industries

- ⌘ Global competitiveness may eventually require *compliance*
  - ⌘ Voluntary use of 7799-2 in the EU
  - ⌘ Could we help US businesses compete globally?
- ⌘ False sense of security?

# How to get involved

Revision process:

¥ US TAG developing comments *now*

¥ October 7th — 15<sup>th</sup>: National Bodies review and vote on proposed changes

¥ Path forward developed

¥ Resolving comments in working group meetings likely through 2003

# How to get involved

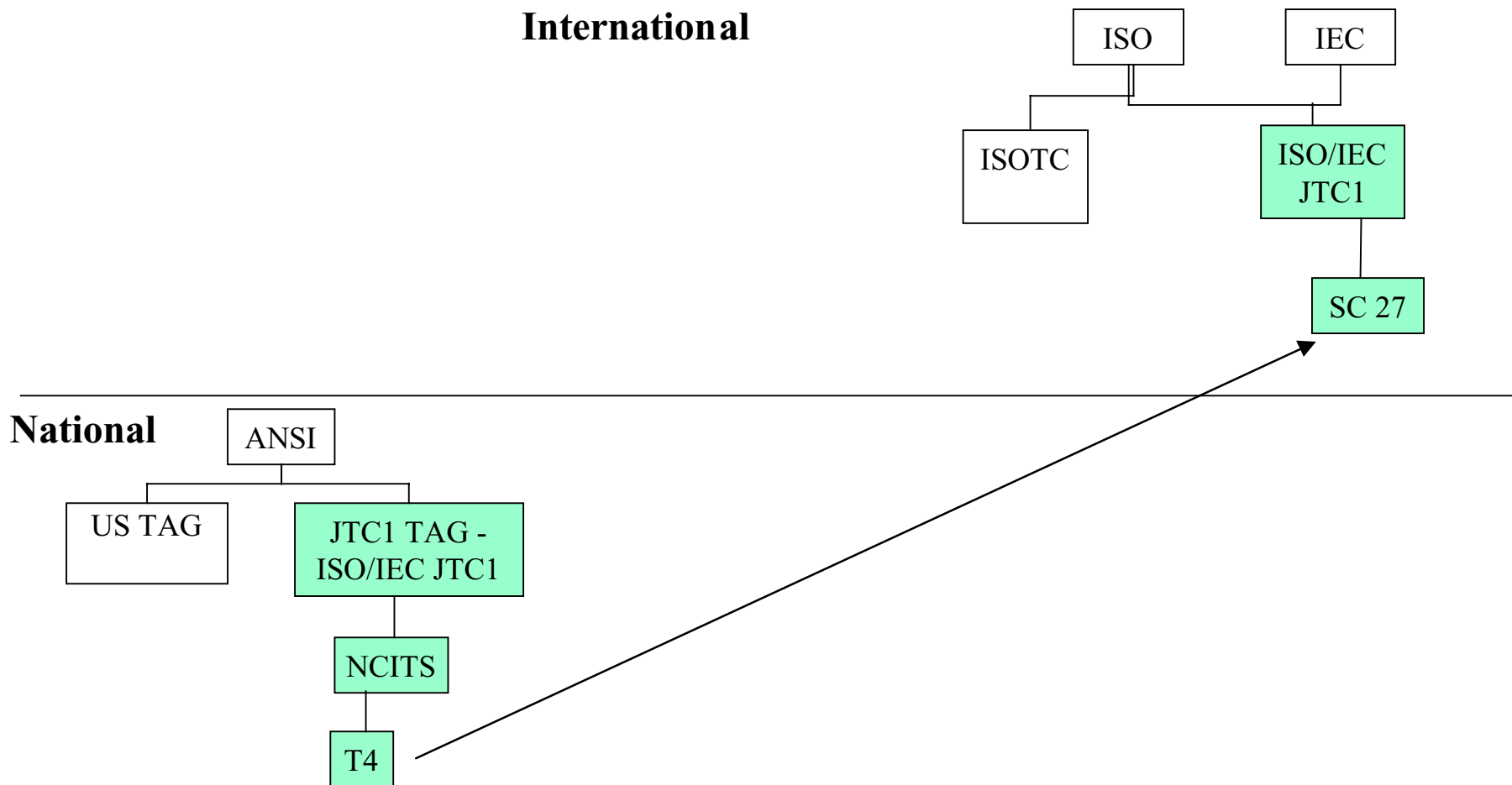
Join T4, the US TAG to  
ISO/IEC JTC 1 SC  
27, IT Security  
Techniques

---

Rowena Chester, Chair  
PO Box 7105  
Oak Ridge, TN 37830  
Phone (865)435-7114  
Fax (865)435-4835  
Email: roc2@cornell.edu

Lucent Technologies  
Griffin Consulting  
HP Computer Corp.  
MCS, Inc.  
National Institute of Standards  
and Technology  
National Security Agency  
RSA Security  
SHARE Inc.  
Six Continents Hotels  
Software Productivity  
Consortium  
Surety Technologies, Inc.  
Tenn. Secure Data Systems

# National → International Bodies



# T4 Structure

≠ **T4 informally shadows SC 27 s structure with 3 WGs**

≠ WG 1 - Requirements, security services, guidelines

≠ WG 2 - Security techniques and mechanisms

≠ WG 3 - Security evaluation criteria

# T4 s Work Includes

- ∕ **Standardization of generic methods for information technology security.**
  - identification of generic requirements for IT system security services,
  - ∕ development of security techniques and mechanisms
- ∕ **Development of security guidelines,**
- ∕ **Development of management support documentation and standards**

# T4 Projects

∞A framework for IT security assurance

∞Digital signatures

∞Modes of operation for an n-bit block cipher

∞Entity authentication

∞Evaluation criteria for IT Security - Part 2: Security functional requirements

∞Guide on the production of protection profiles and security targets

∞Guidelines for the implementation, operation and management of intrusion detection systems (IDS)

∞Key management

∞Methodology for IT security evaluation

For a complete list of T4 projects and their status and review schedules see:

[http://www.ncits.org/tc\\_home/t4htm/index.html](http://www.ncits.org/tc_home/t4htm/index.html)

click on list of projects

# To Make Technical Contributions

Join T4, the US TAG to ISO/IEC JTC 1 SC 27,  
IT Security Techniques

---

Rowena Chester, Chair

PO Box 7105

Oak Ridge, TN 37830

Phone (865)435-7114

Fax (865)435-4835

Email: [roc2@cornell.edu](mailto:roc2@cornell.edu)