Case Number: 2019-0203-F

FOIA MARKER

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

Folder Title: NIISS [National Information Infrastructure Security Group]-Standards				
Staff Office-Individual: Strategic Planning-Bobbitt, Philip				
Original OA/ID Number: 1751				
Row: 49	Section: 1	Shelf: 11	Position: 3	Stack: V

Facsimile Transmission Cover Sheet

cc, Bob Kolt
Wechsler

Critical Infrastructure Assurance Office

PO Box 46258
Washington, DC 20050-6258
Phone: (703) 696-9395
Fax: (703) 696-9410/11

To: DICK CLARKE / THEIR ROBERTS

Phone:

Fax: 202 456-9360

From:

Ext:

Comments: DRAFT OF STANDARDS PRESENTATION
FOR ADVISORY COMMITTEE.
PLEASE CALL/FAX WITH COMMENTS!

Number of pages including this page:

DRAFT

National Institute of Information Systems Standards:

Role of Standards

- Why standards?
  - Basis for interchangeability
  - Metrics for security/protection for products/systems
  - Certification of minimum capability (e.g. cyber-security services)
  - Framework for technological development and best practices sharing
- Definitions
  - Standards - approved documented and available set of criteria used to establish adequacy of an action or object
  - Certification - comprehensive assessment of security features/safeguards to establish whether a system meets specified requirements
  - Best practices - like a "snapshot" of practices that can be relied on until standards are available

National Institute of Information Systems Standards: Role of Standards *(cont'd)*

- Developing standards and certification involves
  - Government (commerce-NIST, NSA)
  - Industry - suppliers, users
  - Standards organizations (ANSI, IEEE, ICSA)
  - International players
- Eclectic process in US
- Many standards - but not widely used
  - ISC2 certifies professional qualifications of information systems security personnel

DRAFT

National Institute of Information Systems Standards:

On-Going Efforts

Past/current efforts

- Orange book criteria
- Common criteria
  - — International agreement
  - — Certified private laboratories for evaluation

Lessons learned

- Systems, not standalone products
- Rated products are behind the technology
  - — Users prefer technology over security
- Lacked community and government buy-in
- Developers lacked "best practices" to facilitate the process
- Lack of understanding of what it really meant

DRAFT

National Institute of Information Systems Standards:

Influence of Standards

- Avoidance of legal liability
  - — Compliance with standards would reflect due diligence
- Insurance coverage
  - — Standards would establish insurable criteria
- Vulnerability assessments
  - — Facilitate assessments
  - — Assist in determining whether reasonable precautions have been taken
- Universality
  - — Basis for widespread use

DRAFT

National Institute of Information Systems Standards:

Creating the National Center

- Create/elevate one or more laboratories to:
  - Accredit cyber-security service providers
  - Develop/promulgate standards for evaluating security
  - Accredit other laboratories to do software/hardware/systems evaluations against standards
  - Focus research agenda
- Initial government support - subsequent spin-off to industry
  - Underwriters laboratory model

National Institute of Information Systems Standards:

Role of Standards

- Why standards?
  - Basis for interchangeability
  - Metrics for security/protection for products/systems
  - Certification of minimum capability (e.g. cyber-security services)
  - Framework for technological development and best practices sharing
- Definitions
  - Standards - approved documented and available set of criteria used to establish adequacy of an action or object
  - Certification - comprehensive assessment of security features/safeguards to establish whether a system meets specified requirements
  - Best practices - like a "snapshot" of practices that can be relied on until standards are available

National Institute of Information Systems Standards: Role of Standards *(cont'd)*

- Developing standards and certification involves
  - Government (commerce-NIST, NSA)
  - Industry - suppliers, users
  - Standards organizations (ANSI, IEEE, ICSA)
  - International players
- Eclectic process in US
- Many standards - but not widely used
  - ISC2 certifies professional qualifications of information systems security personnel

DRAFT

National Institute of Information Systems Standards:

On-Going Efforts

Past/current efforts

- Orange book criteria
- Common criteria
  - — International agreement
  - — Certified private laboratories for evaluation

Lessons learned

- Systems, not standalone products
- Rated products are behind the technology
  - — Users prefer technology over security
- Lacked community and government buy-in
- Developers lacked "best practices" to facilitate the process
- Lack of understanding of what it really meant

National Institute of Information Systems Standards:

Influence of Standards

- Avoidance of legal liability
  - — Compliance with standards would reflect due diligence
- Insurance coverage
  - — Standards would establish insurable criteria
- Vulnerability assessments
  - — Facilitate assessments
  - — Assist in determining whether reasonable precautions have been taken
- Universality
  - — Basis for widespread use

National Institute of Information Systems Standards:

Creating the National Center

- Create/elevate one or more laboratories to:
  - Accredit cyber-security service providers
  - Develop/promulgate standards for evaluating security
  - Accredit other laboratories to do software/hardware/systems evaluations against standards
  - Focus research agenda
- Initial government support - subsequent spin-off to industry
  - Underwriters laboratory model

National Institute of Information Systems Standards:

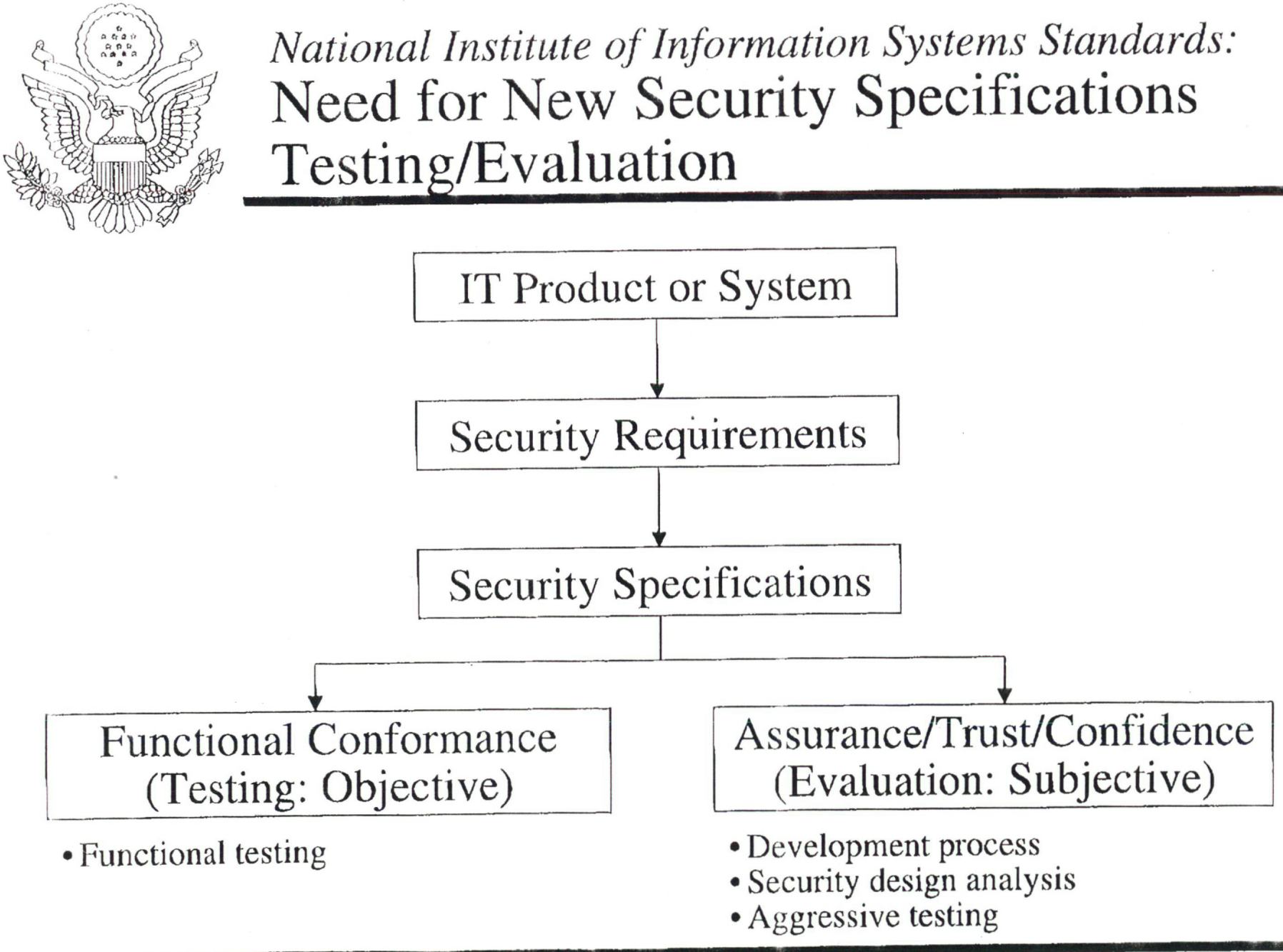
Creating the National Center *(cont'd)*

- Issues
  - — Industry support - from providers?
    from customers?
    from third parties (e.g. insurance)?
  - — R&D challenges
  - — Keeping standards current

- Next steps: consultation with private sector

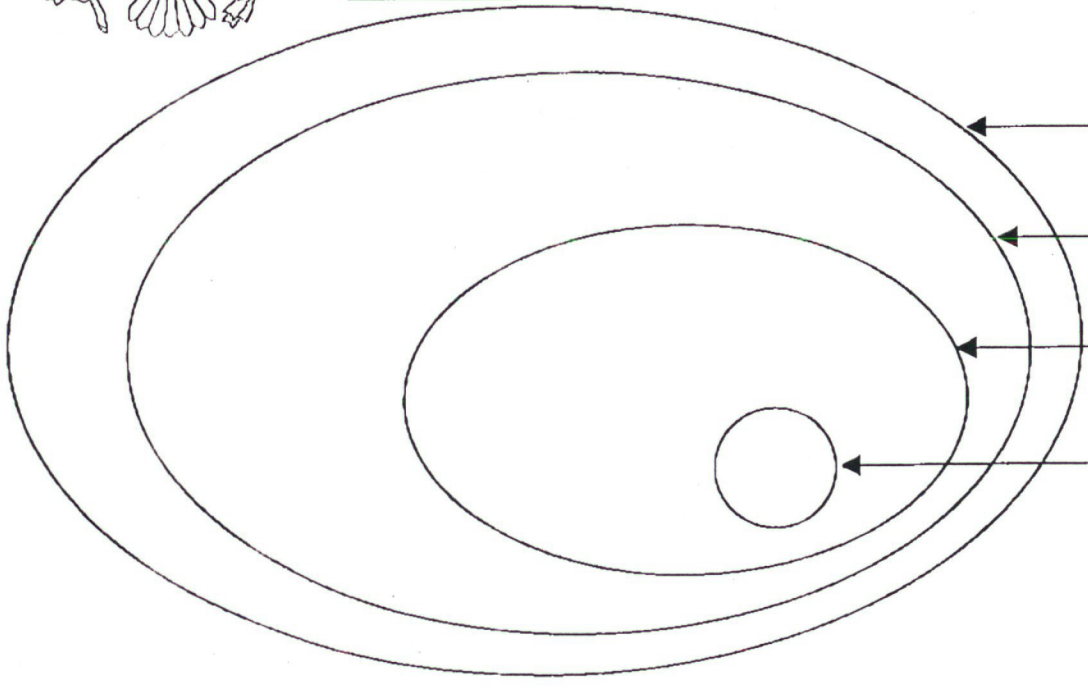
National Institute of Information Systems Standards:

Need for New Security Specifications Testing/Evaluation



National Institute of Information Systems Standards:

Need for System Standards



Level	Examples	Specification
Application/system	Air traffic control	CC, GSSP, ...
Product	Firewall, OS	Common criteria (CC)
Security module	Crypto module	FIPS 140-1
Algorithm	DES	FIPS 46-2