in050057

InterNational Committee for Information Technology Standards
INCITS Secretariat, Information Technology Industry Council (ITI)
1250 Eye St. NW, Suite 200, Washington, DC 20005
Telephone 202-737-8888; Fax 202-638-4922;
Email: incits@itic.org

ACTION REQUESTED

Date:	January 26, 2005
Due Date:	**February 21, 2005**
Attachment:	in041508R
Reply to:	Jennifer Garner
Phone:	(202) 626-5737
Email:	jgarner@itic.org

To:	INCITS/T4
Subject:	**Request for INCITS/T4 Input on the Proposal of the INCITS Ad Hoc on Cyber Security to Establish a New INCITS Technical Committee, INCITS/CS1 - Cyber Security, and Designate INCITS/CS1 as the US TAG for JTC 1/SC 27 and all SC 27 Working Groups Except SC 27/WG 2** - Action Item 26 from the January 2005 INCITS Executive Board Meeting

Background

At the September 2004 meeting of the INCITS Executive Board, the INCITS Ad Hoc on Cyber Security was established to conduct an inventory activity on existing Cyber Security standardization and to aggressively pursue new work on Cyber Security.

The recommendation of the INCITS Ad Hoc on Cyber Security (in041508R - attached) was reviewed at the January 20, 2005 meeting of the INCITS Executive Board, and the following motion was approved:

> Move to initiate a 30-day INCITS Executive Board letter ballot of document in041508 as revised at January 2005 Executive Board meeting, INCITS Ad Hoc Group on Cyber Security Recommendation to Establish a New INCITS Technical Committee on Cyber Security, with the following instructions:
>
> 1. Document in041508 as revised at January 2005 EB meeting is immediately forwarded by the INCITS Secretariat to INCITS T4 for their review at their February 16-17, 2005 meeting.
>
> 2. Immediately after the February 16-17, 2005 INCITS T4 meeting, the 30-day INCITS EB letter ballot of document in041508 as revised at January 2005 EB meeting is issued, with any comments by INCITS T4 attached.

If the letter ballot passes:

1. The INCITS Secretariat will issue the required notices of the formation of the new INCITS Technical Committee on Cyber Security, as well as calls for participation and contributions.

2. The INCITS Secretariat will appoint an interim chair for the first meeting of the new INCITS Technical Committee on Cyber Security.

3. The first meeting of the new INCITS Technical Committee on Cyber Security would take place in the Washington, DC area. The first meeting would be scheduled for a maximum of two and half days (tentative dates: Wednesday to Friday, May 25-27, 2005).

4. After the close of the first meeting, the assignment of the US TAG for ISO/IEC JTC 1/SC 27 and SC 27 WGs 1 and 3 would be transferred from INCITS T4 to the new INCITS Technical Committee on Cyber Security. The SC 27/WG 2 TAG assignment will be retained by INCITS/T4.

Requested Action

Document in041508R (attached) is submitted for consideration at the February 16-17, 2005 INCITS/T4 meeting. INCITS/T4 is invited to provide input, by February 21, 2005, for consideration by the INCITS Executive Board during the letter ballot on approval of in041508R. The INCITS/T4 input should be sent to Jennifer Garner (jgarner@itic.org) by **February 21, 2005**.

in041508R

January 20, 2005

To: INCITS Executive Board

From: INCITS Ad Hoc Group on Cyber Security

Subject: Recommendation to Establish a New INCITS Technical Committee on Cyber Security

Introduction

Cyber security is now one of the highest priorities for organizations and individuals. This is because of the ubiquity of Information Technology, which spans all aspects of business, commerce, and government. An organization's IT infrastructure has to be secure so that everything else can be secure. Cyber security is a key component of post September 11th priorities for the security of critical infrastructure. Cyber security is dependent upon sound and comprehensive national and international consensus standards.

Recent reports have highlighted the critical importance and priority of cyber security and cyber security standards. The recommendations of the National Cyber Security Partnership's (NCSP) Technical Standards and Common Criteria Task Force[1] identify the spectrum of cyber security standards that will be needed to maintain the confidentiality, integrity and availability of computers, networks and most importantly the information therein. The ISO Advisory Group on Security (AGS)[2] has recognized the central importance of cyber security and will recommend that ISO/IEC JTC 1/ SC 27, IT Security Techniques, take a top down proactive approach to ensure that all aspects of cyber security standardization are being progressed in a timely fashion.

There are other efforts underway to standardize various aspects of information security and information security management. NIST has been mandated to develop such standards for US Federal systems that are sensitive but not classified. Standards mandated for Federal government systems are well positioned to become sources for national standards as there are many "private" systems who chose to or who are required to meet Federal requirements. Many of the documents being developed by NIST are being used in IEEE Project 1700, Standard for Information System Security Assurance Architecture. The ISSAA is intended to provide a comprehensive process model for the cost-effective selection, documentation, implementation, and assessment of security controls for an information system; and for making and maintaining system security accreditation decisions. It would be advantageous to all stakeholders, national and

[1] http://www.cyberpartnership.org/TF4TechReport.pdf

[2] http://public.ansi.org/ansionline/Documents/Standards%20Activities/Homeland%20Security%20Standards%20Panel/ANSI-HSSP%20Third%20Plenary/Day%202%20Presentations/Arnold.ppt

international, if this work by IEEE were eventually submitted by the US to ISO/IEC JTC 1/ SC 27 for international consideration.

As the US TAG to ISO/IEC JTC 1, INCITS has the responsibility for developing international standards for cyber security as well as counterpart national standards. Keeping national and international cyber security standards, especially information security management standards, consistent should be a strategic goal of INCITS. Such harmonization helps US industries to be competitive globally and increases the chances of being able to secure cyberspace, which knows no national boundaries.

With all of the present focus on the importance of cyber security standardization, there is a clear need to elevate INCITS role in this work. Presently, the BSI (UK) is the driving force within ISO/IEC JTC 1/ SC 27 Working Group 1 where the work on Information Security Management Systems (ISMS) is being pursued. INCITS needs to become proactive in national and international system security standardization, not just cryptography standardization. Given the global nature and practices of many US companies, the development of national standards can be an effective means of fostering international as well as national consensus and adoption before formally introducing the material into the international standardization process.

Existing Situation in INCITS

Presently, INCITS has four technical committees involved, to one degree or another, with cyber security standardization. INCITS T3 is responsible for ISO/IEC 9594 (ITU-T X.509). This standard is used by major suppliers of directory services as foundation for Lightweight Directory Access Protocol (LDAP) access to such services in the Internet and is becoming a key enabler for secure authentication in networked applications. INCITS B10 is now developing comprehensive national and international standards for interoperability of smart cards. Applications for smart card technologies include travel documents (e.g., passports), identification badges (e.g., employees, students), and credit/debit cards. INCITS M1 is rapidly developing comprehensive national and international standards for biometrics. Together, these standards for the interoperability of smart card and biometric technologies will support highly secure physical and logical access control applications.

The INCITS technical committee with the broadest cyber security scope is INCITS T4. With only about 14 members, T4 has, in practice, opted to not develop national standards in this area. T4 is primarily focused on developing security techniques and mechanisms within ISO/IEC JTC 1/SC 27 WG 2 (Security techniques and mechanisms). T4 contributions to the international work of ISO/IEC JTC 1/SC 27 WG 1 (Requirements, security services and guidelines) and WG 3 (Security evaluation criteria) have largely come from only 3 or 4 of the T4 members. As such, T4 has been unable to maintain a proactive and diverse representation of stakeholders for the standardization of the broad range of topics presently within its scope.

A new INCITS TC for Cyber Security has the potential for drawing large numbers of diverse stakeholders with relevant expertise that could be focused on priority standards development. The new INCITS TC would be responsible for developing cyber security standards aimed at maintaining the confidentiality, integrity and availability of computers, networks and most importantly the information therein.

Recommendation - Establishment of a New INCITS Technical Committee on Cyber Security

The INCITS Ad Hoc Group on Cyber Security recommends that INCITS establish a new INCITS Technical Committee for Cyber Security, INCITS CS1, and designate INCITS CS1 as the US TAG for ISO/IEC JTC 1/SC 27 and all SC 27 Working Groups except WG 2 (INCITS/T4 will serve as the US TAG to SC 27/WG 2). The INCITS CS1 area of work would include standardization in the following areas:

1. Management of information security and systems
2. Management of third party information security service providers
3. Intrusion detection
4. Network security
5. Incident handling
6. IT Security evaluation and assurance
7. Security assessment of operational systems
8. Security requirements for cryptographic modules
9. Protection profiles
10. Role based access control
11. Security checklists
12. Security metrics

The scope of the new INCITS CS1, Cyber Security, would explicitly exclude the areas of work on cyber security standardization presently underway in INCITS B1, M1 and T3; as well as other standard groups, such as ATIS, IEEE, IETF, TIA, and X9. INCITS T4's area of work would be narrowed to cryptography projects in ISO/IEC JTC 1/SC 27 WG 2 (Security techniques and mechanisms).

Attachments

Attached is a listing of organizations, which may be likely to participate in INCITS CS1, Cyber Security.

Members of the INCITS Ad Hoc Group on Cyber Security have begun informally trying to ascertain interest in specific projects for the proposed new TC. Also attached are some initial sample project proposals. It is anticipated that more details on the proposing organizations for these proposals, and more project proposals, will be available within the next few weeks.

Prospective Members of the New INCITS TC for Cyber Security

Based upon information reviewed by the INCITS Ad Hoc Group on Cyber Security, the following organizations were identified as prospective members for a new INCITS Technical Committee on Cyber Security:

Bank of New York
Bell Labs Lucent Technologies
BITS
Bronson Healthcare Group
Cable and Wireless
Capehart Associates LLC
Center for Internet Security
Check Point Software Technologies
Cisco Systems
Computer Sciences Corporation (CSC)
Corsec Security
Decisive Analytics Corporation
DeepNines Technologies
Deer Run Associates
Department of Defense
Department of Homeland Security
Department of the Navy
EDS
EWA-Canada
Georgia Tech Research Institute
Harris Corporation
IBM
Internet Security Systems
Intrado
Juniper Networks
Logica
Marconi Wireless
Microsoft Corporation
Network Associates
NIST
Nortel
NSA
Oracle Corporation
Phoenix Technologies, Ltd.
ProMedica Health System
Purdue University
SAIC
St. Joseph's University
Sun Microsystems, Inc.
Symantec Corporation
Syntegra
The Dow Chemical Company
United States Navy, COMPACFLT
University of Maryland, Baltimore County
VPN Consortium
webMethods
Zone Labs, Inc.

Sample Project Proposals for the New INCITS TC for Cyber Security

Draft Project Proposal # 1

Role Based Access Control (RBAC) Profile for Health Care Applications

1. Source of the Proposed Project

1.1. Title

Role Based Access Control (RBAC) Profile for Health Care Applications

1.2. Date Submitted

To Be Determined (TBD)

Date of this draft: December 21, 2004

1.3. Proposer

Mike Davis, Department of Veterans Affairs (SAIC), Rick Kuhn, NIST

2. Process Description for the Proposed Project

2.1. Project Type

D - this is a standard development project.

2.2. Type of Document

The project is expected to result in an ANSI/INCITS standard.

2.3. Definitions of Concepts and Special Terms

Base Standards - define fundamentals and generalized procedures. They provide an infrastructure that can be used by a variety of applications, each of which can make its own selection from the options offered by them.

Application Profiles - define conforming subsets or combinations of base standards used to provide specific functions. Application Profiles identify the use of particular options available in the base standards, and provide a basis for the interchange of data between applications and interoperability of systems.

2.4. Expected Relationship with Approved Reference Models, Architectures, etc.

None

2.5. Recommended INCITS Development Technical Committee

It is recommended that a new INCITS Technical Committee for Cyber Security be established to do this work.

2.6. Anticipated Frequency and Duration of Meetings

It is anticipated that this project would require one-day meetings approximately four times annually.

2.7. Target Date for Initial Public Review

If a new INCITS Technical Committee for Cyber Security is established by INCITS in January 2005, it is estimated that the draft document would be ready for submission to INCITS for Milestone 4 processing in March 2006.

2.8. Estimated Useful Life of Standard

There is no known limitation on the useful life of this proposed standard.

3. Business Case for Developing the Proposed Standard

3.1. Description

This proposed RBAC Profile will define the functional requirements for role based access control in health care applications. It will specify the use of existing requirements and/or options in the relevant base standard in order to provide for the interoperability of role based access in health care systems. The base standard that will be profiled is INCITS 359-2004, American National Standard for Information Technology - Role Based Access Control.

3.2. Existing Practice and the Need for a Standard

Currently, there is no profile standard addressing role based access control in health care applications. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), also known as Public Law 104-191, establishes requirements for the protection of health records and related information. HIPAA regulations specifically cite RBAC as the desired security model for health records, and providers have a need to store and exchange records securely. Standards for RBAC in health care are needed to ensure interoperability among health care applications and meet privacy requirements of HIPAA and related rules.

3.3. Implementation Impacts of the Proposed Standard

3.3.1. Development Costs

Since relevant work has already been performed within existing standards groups and federal agencies, it is expected that the costs related to further development of this profile would be low.

Technical editor labor is expected to total about two months of a staff-year.

3.3.2. Impact on Existing or Potential Markets

Existing and new markets for RBAC systems should experience added impetus from the benefits of interoperability. Development of this standard should help to further accelerate the deployment of standards-based RBAC applications within health care systems.

3.3.3. Costs and Methods for Conformity Assessment

The possible testing environment may range from the use of suppliers' declarations to third party testing. Therefore, the cost of conformity assessment is not known at this time.

3.3.4. Return on Investment

There is no known data on which to make an estimate.

3.4. Legal Considerations

3.4.1. Patent Assertions

INCITS 359-2004, American National Standard for Information Technology - Role Based Access Control, will be the base standard profiled. There are no known patents relevant to this standard.

3.4.2. Dissemination of the Standard

Drafts of this standard will be distributed electronically. There may be distribution constraints as this document reaches different stages of development and processing within INCITS. There are no known IPR issues.

4. Related Standards Activities

4.1. Existing Standards

INCITS 359-2004, American National Standard for Information Technology - Role Based Access Control

4.2. Related Standards Activity

- This proposed standard is expected to be compatible with the Core and Hierarchical Role Based Access Control (RBAC) profile of XACML, Version 2.0 (Committee Draft 01, 11 November 2004) developed by OASIS XACML TC.

- IETF RFC 3881 is a basic reference document for the Integrating the Healthcare Enterprise (IHE) "Audit Trail and Node Authentication" profile and DICOM Supplement 95.

4.3. Recommendations for Close Liaison

INCITS Technical Committees B10 and M1

OASIS XACML Technical Committee

5. Units of Measurement used in the Standard

Indicate units of measurement used in the Standard:

- ___ International Systems of Units (SI)
- ___ Inch/Pound
- ___ Both
- ___ Other
- **XX** Not Measurement Sensitive

It is not anticipated that units from a physical dimensioning system will be needed for specifying the requirements of this standard. If necessary, the goal would be to use the International System of Units (SI).

Draft Project Proposal # 2

Security Metrics for IT Systems

1. Source of the Proposed Project

1.1. Title

Security Metrics for IT Systems

1.2. Date Submitted

To Be Determined (TBD)

Date of this draft: December 21, 2004

1.3. Proposer

TBD

2. Process Description for the Proposed Project

2.1. Project Type

D - this is a standard development project.

2.2. Type of Document

The project is expected to result in an ANSI/INCITS standard.

2.3. Definitions of Concepts and Special Terms

Security Metrics – tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

2.4. Expected Relationship with Approved Reference Models, Architectures, etc.

None

2.5. Recommended INCITS Development Technical Committee

It is recommended that a new INCITS Technical Committee for Cyber Security be established to do this work.

2.6. Anticipated Frequency and Duration of Meetings

It is anticipated that this project would require one-day meetings approximately four times annually.

2.7. Target Date for Initial Public Review

If a new INCITS Technical Committee for Cyber Security is established by INCITS in January 2005, it is estimated that the draft document would be ready for submission to INCITS for Milestone 4 processing in March 2006.

2.8. Estimated Useful Life of Standard

There is no known limitation on the useful life of this proposed standard.

3. Business Case for Developing the Proposed Standard

3.1. Description

The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in these activities by applying corrective actions based on observed measurements. The requirement to measure IT security performance is driven by regulatory, financial, and organizational reasons.

Possible security metrics cover a vast range of measurable items. However, as the definition implies, security metrics do not represent a singular numeric reference, but instead represent data collected and analyzed over time. The goals of security metrics include identifying security weaknesses to improve the overall security posture, determining trends to better utilize the ever decreasing security budget, and measuring the success (or failure) of implemented security solutions. Ultimately, the metrics should accurately portray the overall organization security posture from a risk/threat, budgetary, and regulatory standpoint.

3.2. Existing Practice and the Need for a Standard

A number of existing laws, rules, and regulations cite IT performance measurement in general and IT security performance measurement in particular, as a requirement. These include the Clinger-Cohen Act, Government Performance and Results Act (GPRA), Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA). Currently, organizations measure the performance and security of their IT systems in a variety of qualitative and quantitative ways without wide consensus on best practices for describing a system's security posture.

A security metrics program provides a number of organizational and financial benefits. With standard security metrics, an organization can improve accountability, pinpoint specific technical, operational, or management controls that are not being implemented, are implemented incorrectly or are ineffective in their implementation. Program managers and system owners can use data collected to target and justify security investments and relate results of security activities to respective requirements. With consensus based standards on how to describe one's security posture, organizations will also be better equipped to make fact based decisions when connecting information systems. The National Cyber Security Partnership Technical Standards and Common Criteria Task Force recommended that industry work together to develop a defined set of standards for determining the security level or security status of cyberspace in support of the President's National Strategy to Secure Cyberspace.

3.3. Implementation Impacts of the Proposed Standard

3.3.1. Development Costs

Since relevant work is currently underway within NIST, it is expected that the costs related to further development of this standard would be low.

Technical editor labor is expected to total about two months of a staff-year.

3.3.2. Impact on Existing or Potential Markets

Development of this standard should help to further accelerate the safe interconnection of IT systems, system reliability, and the increase of end user trust and confidence in IT systems. This in turn could have a great impact on e-commerce and the uptake of more ubiquitous IT solutions.

3.3.3. Costs and Methods for Conformity Assessment

The possible testing environment may range from the use of suppliers' declarations to third party testing. Therefore, the cost of conformity assessment is not known at this time.

3.3.4. Return on Investment

There is no known data on which to make an estimate.

3.4. Legal Considerations

3.4.1. Patent Assertions

There are no known patents relevant to this standard development project.

3.4.2. Dissemination of the Standard

Drafts of this standard will be distributed electronically. There may be distribution constraints as this document reaches different stages of development and processing within INCITS. There are no known IPR issues.

4. Related Standards Activities

4.1. Existing Standards

There are no known existing standards.

4.2. Related Standards Activity

- NIST Special Publication 800-55: Security Metrics for Information Technology Systems
- NIST DRAFT Special Publication 800-53A: Guide for Assessing the Security Controls in Federal Information Systems (to become Federal Information Processing Standard (FIPS) 200 by December 2005)

4.3. Recommendations for Close Liaison

There are no liaison recommendations at this time.

5. Units of Measurement used in the Standard

Indicate units of measurement used in the Standard:

- ___ International Systems of Units (SI)
- ___ Inch/Pound
- ___ Both
- ___ Other
- **XX** Not Measurement Sensitive

It is not anticipated that units from a physical dimensioning system will be needed for specifying the requirements of this standard. If necessary, the goal would be to use the International System of Units (SI).

Project Proposal # 3

Protection Profile for Firewalls

1. Source of the Proposed Project

1.1. Title

Protection Profile for Firewalls

1.2. Date Submitted

To Be Determined (TBD)

Date of this draft: December 21, 2004

1.3. Proposer

TBD

2. Process Description for the Proposed Project

2.1. Project Type

D- this is a standard development project.

2.2. Type of Document

The project is expected to result in an ANSI/INCITS standard.

2.3. Definitions of Concepts and Special Terms

Protection Profile – an implementation independent set of security requirements for a category of IT products, which meet specific consumer needs.

Firewall - A functional unit that mediates all traffic between two computer networks and protects one of them or some part thereof against unauthorized access. The protected network is in general a private, internal network. A firewall may permit messages or files to be transferred to a high-security workstation within the internal network, without permitting such transfer in the opposite direction.

2.4. Expected Relationship with Approved Reference Models, Architectures, etc.

None

2.5. Recommended INCITS Development Technical Committee

It is recommended that a new INCITS Technical Committee for Cyber Security be established to do this work.

2.6. Anticipated Frequency and Duration of Meetings

It is anticipated that this project would require one-day meetings approximately four times annually.

2.7. Target Date for Initial Public Review

If a new INCITS Technical Committee for Cyber Security is established by INCITS in January 2005, it is estimated that the draft document would be ready for submission to INCITS for Milestone 4 processing in March 2006.

2.8. Estimated Useful Life of Standard

There is no known limitation on the useful life of this proposed standard.

3. Business Case for Developing the Proposed Standard

3.1. Description

The purpose of creating protection profiles (PPs), standards against which products can be tested, is to provide technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems and hence increase consumer trust in cost-effective ways.

3.2. Existing Practice and the Need for a Standard

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative originated to meet the security testing needs of both information technology (IT) consumers and producers. Under NIAP, the Protection Profile Review Board validates US Government Protection Profiles. These profiles are validated based upon the process under which they are developed and conformance to a specified robustness. Security experts in public and private sector have noted that protection profiles could be better suited for generalized use and critical infrastructure protection if the profiles were developed with realistic requirements under consensus between public and private sector. The National Cyber Security Partnership (NCSP) Technical Standards and Common Criteria Task Force has suggested that performance and interoperability testing could complement PPs requirements to satisfy customers' security needs and that all PPs should include vulnerability assessments against a standard set of vulnerability tests.

The NCSP Technical Standards and Common Criteria Task Force suggested that consensus based requirements in the form of PPs could be used in support of the President's National Strategy to Secure Cyberspace. Protection Profiles have generally been written for system components. Therefore one would expect separate standards for each protection profile with the appropriate expertise gathered to ensure its efficacy.

3.3. Implementation Impacts of the Proposed Standard

3.3.1. Development Costs

Relevant work is currently underway within NIST to develop protection profiles for firewalls, VPNs, and routers. Therefore, it is expected that the costs related to further development of this protection profile would be low.

Technical editor labor is expected to total about two months of a staff-year.

3.3.2. Impact on Existing or Potential Markets

Development of standard protection profiles should help to further assure the security of networks. This in turn could have a great impact on e-commerce and the uptake of more ubiquitous IT solutions.

3.3.3. Costs and Methods for Conformity Assessment

The possible testing environment may range from the use of suppliers' declarations to third party testing. Therefore, the cost of conformity assessment is not known at this time.

3.3.4. Return on Investment

There is no known data on which to make an estimate.

3.4. Legal Considerations

3.4.1. Patent Assertions

There are no known patents relevant to this standard.

3.4.2. Dissemination of the Standard

Drafts of this standard will be distributed electronically. There may be distribution constraints as this document reaches different stages of development and processing within INCITS. There are no known IPR issues.

4. Related Standards Activities

4.1. Existing Standards

ISO/IEC TR 15446, Guide on the production of Protection Profiles and Security Targets.

4.2. Related Standards Activity

There is no known related standards activity.

4.3. Recommendations for Close Liaison

There are no liaison recommendations at this time.

5. Units of Measurement used in the Standard

Indicate units of measurement used in the Standard:

- ___ International Systems of Units (SI)
- ___ Inch/Pound
- ___ Both
- ___ Other
- **XX** Not Measurement Sensitive

It is not anticipated that units from a physical dimensioning system will be needed for specifying the requirements of this standard. If necessary, the goal would be to use the International System of Units (SI).

Project Proposal # 4

Risk Based Information Security Management

1. Source of the Proposed Project

1.1. Title

Risk Based Information Security Management

1.2. Date Submitted

To Be Determined (TBD)

Date of this draft: December 21, 2004

1.3. Proposer

TBD

2. Process Description for the Proposed Project

2.1. Project Type

D - this is a standard development project.

2.2. Type of Document

The project is expected to result in an ANSI/INCITS standard.

2.3. Definitions of Concepts and Special Terms

None

2.4. Expected Relationship with Approved Reference Models, Architectures, etc.

None

2.5. Recommended INCITS Development Technical Committee

It is recommended that a new INCITS Technical Committee for Cyber Security be established to do this work.

2.6. Anticipated Frequency and Duration of Meetings

It is anticipated that this project would require one-day meetings approximately four times annually.

2.7. Target Date for Initial Public Review

If a new INCITS Technical Committee for Cyber Security is established by INCITS in January 2005, it is estimated that the draft document would be ready for submission to INCITS for Milestone 4 processing in March 2006.

2.8. Estimated Useful Life of Standard

There is no known limitation on the useful life of this proposed standard.

3. Business Case for Developing the Proposed Standard

3.1. Description

This standard would provide a comprehensive process model for the cost-effective documentation, implementation, and assessment, of security controls for an information system.

3.2. Existing Practice and the Need for a Standard

A number of existing laws, rules, and regulations cite IT performance measurement in general and IT security performance measurement in particular, as a requirement. These include the Clinger-Cohen Act, Government Performance and results Act (GPRA), Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA). Currently, organizations evaluate and improve the performance and security of their IT systems in a variety of ways without wide consensus on best practices for information security management.

An ISO/IEC project has begun to develop an information security management system standard. It has been proposed that this standard be designed as an umbrella standard that points to numerous additional documents. Work in progress at NIST and within IEEE offer a simpler, more effective alternative to the scheme being discussed on the international level. The US could better influence the international work by bringing a national standard to the international discussions.

3.3. Implementation Impacts of the Proposed Standard

3.3.1. Development Costs

Relevant work is currently underway within NIST to develop a series of standards, which collectively will be used to manage Federal information systems. Many of the documents within this family are already in use by public and private sector. It is expected, therefore, that the costs related to further development of this profile would be low.

Technical editor labor is expected to total about two months of a staff-year.

3.3.2. Impact on Existing or Potential Markets

An ISO/IEC project has begun to develop an information security management system standard. It has been proposed that this standard be designed as an umbrella standard that points to numerous additional documents. Work in progress at NIST and within IEEE offer a simpler, more effective alternative to the scheme being discussed on the international level. The US could better influence the international work by bringing a national standard to the international discussions. An international standard for risk based information security management that's consistent with the standards mandated for US federal systems and in wide us by US private sector would greatly impact US competitiveness on a global level.

3.3.3. Costs and Methods for Conformity Assessment

The possible testing environment may range from the use of suppliers' declarations to third party testing. Therefore, the cost of conformity assessment is not known at this time.

3.3.4. Return on Investment

There is no known data on which to make an estimate.

3.4. Legal Considerations

3.4.1. Patent Assertions

There are no known patents relevant to this standard.

3.4.2. Dissemination of the Standard

Drafts of this standard will be distributed electronically. There may be distribution constraints as this document reaches different stages of development and processing within INCITS. There are no known IPR issues.

4. Related Standards Activities

4.1. Existing Standards

There are no known existing standards.

4.2. Related Standards Activity

- IEEE Information System Security Assurance Architecture (ISSAA)
- FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems
- FIPS Publication 200: Minimum Security Controls for Federal Information Systems
- NIST Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

- NIST Special Publication 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems
- NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems
- NIST Special Publication 800-53A: Guide for Assessing the Security Controls in Federal Information Systems
- BS 7799- Part 1 and Part 2

4.3. Recommendations for Close Liaison

IEEE Information System Security Assurance Architecture (ISSAA) Working Group.

5. Units of Measurement used in the Standard

Indicate units of measurement used in the Standard:

- ___ International Systems of Units (SI)
- ___ Inch/Pound
- ___ Both
- ___ Other
- **XX** Not Measurement Sensitive

It is not anticipated that units from a physical dimensioning system will be needed for specifying the requirements of this standard. If necessary, the goal would be to use the International System of Units (SI).