

CS1/06-0115

**Revised Project Proposal for INCITS Technical Committee CS1
Minimum Security Guidelines for Protecting Personal Identifiable
Information and other Sensitive Information Stored on and Exchanged
between Information Systems**

1. Source of the Proposed Project

1.1. Title

**Minimum Security Guidelines for Protecting Personal Identifiable
Information and other Sensitive Information Stored on and Exchanged
between Information Systems**

1.2. Date Submitted

3/30/2006

1.3. Proposers

INCITS CS1

2. Process Description for the Proposed Project

2.1. Project Type

DT - A

2.2. Type of Document

The project is expected to result in an ANSI-INCITS Technical Report. In the future, this document may be submitted as an input document to SC 27 since the SC27 WG1 Roadmap has identified a gap for this type of document and there are no current plans in SC27 to produce such a document.

2.3. Definitions of Concepts and Special Terms

Management Controls – Those controls that address the security management aspects of an IT network and its component systems.

Operational Controls – Those controls primarily implemented and executed by people (as opposed to technology) that address the security mechanisms within an IT network and its component systems.

Technical Controls – Those controls that invoke security mechanism contained in and executed by an IT network and its component systems.

Personal Identifiable Information – Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Commonly abbreviated to **PII**.

Sensitive Information – Information that, for business or other reasons, requires protection from loss of confidentiality, integrity, availability, authenticity, reliability, accountability of the information as a result of deletion, misuse, modification, or unauthorized access.

Minimum Security Guidelines – The combination of **Management, Operational,** and **Technical Controls** which provide a minimum baseline level of protection for any organization responsible for the protection of **Personal Identifiable Information** and other Sensitive Information stored on, processed on, and exchanged between an IT network and its component systems.

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

Noting the potential needs of users of the proposed guidelines to have their implementations of IT audited and certificated, the document will establish a set of controls and implementation guidance in the style of ISO/IEC 17799 for the specific scope of any organization that would benefit from a checklist approach to implementing security controls. The primary users of this document would be organizations that do not have access to a security staff focused on defining applicable controls for each control objective in ISO/IEC 17799. However, it is expected that larger organizations would also benefit from these guidelines. The more business, rather than technology, focus of the scope would lead to the new document's clauses being prepared in a form which would allow their easy adoption as a layer of implementation detail which could be readily mapped into an ISMS, however it will not require that the organization also purchase ISO/IEC 27001 or ISO/IEC 17799 as a prerequisite for the implementation of the guidelines in the document. The document will also take into account certain publications in the NIST SP 800 series and incorporate those aspects that apply to the scope of protection of personal identifiable information.

2.5. Recommended INCITS Development Technical Committee

INCITS Technical Committee for Cyber Security.

2.6. Anticipated Frequency and Duration of Meetings

It is anticipated that this project would require one-day meetings approximately three times annually prior to acceptance and two times annually after acceptance.

2.7. Target Date for Initial Public Review

Development of scope and outline:

It is estimated that the draft document will be ready for submission to INCITS for Milestone 4 processing in March 2007.

2.8. Estimated Useful Life of Technical Report

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

3. Business Case for Developing the Proposed Technical Report

3.1. Description

The purpose of establishing these guidelines is to assist organizations that do not have the manpower to evaluate the ISO/IEC 17799 controls and control objectives and produce detailed implementation criteria for those controls. These guidelines would cover organizations such as small and medium businesses responsible for processing, storing, and exchanging **Personal Identifiable Information (PII) and other Sensitive Information** in selecting and applying appropriate controls to protect that information. PII includes sensitive information such as the following:

- Postal address
- E-mail address
- Telephone number
- Social Security Number
- Date of Birth
- Mother's maiden name
- State- or U.S.-issued driver's license or ID number
- Alien registration number
- Passport number
- Employer or tax ID number
- Employment history
- Bank or credit card or debit card account number, and any related PIN
- Medicaid or food stamp account number
- Biometric data
- Unique electronic number, address, or routing code
- Medical records
- Telecommunication ID information or access device
- Other number or information that may be used to access financial resources

Continuing fiduciary, regulatory, financial, and organizational governance requirements of due care all drive the need to establish minimum IT security performance standards that can benefit all organizations, especially those that do not have dedicated security personnel. An immediate, overarching demand for a minimum standard of due care is being driven by numerous State laws requiring public notification when personally identifiable information is inappropriately disclosed. Chief Executives of companies, universities and governments are all asking what they need to do to safeguard that sensitive information. It is incumbent upon the information security community to establish a detailed minimum standard of due care. Possible security standards cover a vast range of measurable items. However, protection of sensitive data on network connected systems can be facilitated by identifying and codifying those minimum steps, regardless of the size of an organization, that have the greatest impact on reducing the probability of loss of sensitive information and the resulting human and financial costs and other consequences.

3.2. Existing Practice and the Need for Guidelines

An increasing flood of identity theft from network-connected computers has resulted in a widespread need for definition of the security practices that meet a minimum standards of due care.

At the same time, a number of existing laws, rules, and regulations have been passed that demand that organizations meet minimum standards for data security. Health care providers and health insurers are subject to the Health Insurance Portability and Accountability Act (HIPAA). Financial organizations are subject to Gramm-Leach-Bliley. Government agencies must improve security under the Federal Information Security Management Act (FISMA). At the same time, standards such as ISO/IEC 27001 and NIST SP 800-53 have been developed. **Each of these guidelines, standards and laws creates high level requirements, but smaller organizations do not always have the breadth of expertise required to determine the level of operational controls required to respond effectively and consistently to the threats incurred by being a member of the cyber community. A document providing specific guidance for implementing a minimum standard of due care for protecting sensitive information can play a major role in reducing identity theft and other compromises of PII and other sensitive information.**

The proposed document is to be a non-banking-oriented document that parallels the PCI Data Security Standard. The proposed document is intended to be fully compatible with the higher level standards, but will add value by focusing on operational controls that directly act to block attacks that would result in PII and other sensitive information being compromised.

Even in the event that an organization chooses not to implement an ISMS *per se*, the proposed document will complement the recognition given to ISO/IEC 17799

as the *de facto* means to protect information systems (ref. Congress, Joint Economic Committee). Users of the proposed document will want to be able to apply it to help them show their compliance with various legislation, some of which is identified above,. The proposed document will, in addition to being harmonized with ISO/IEC 17799, develop a mapping between its specific clauses (i.e. the additional guidance supporting a 17799 control, or new controls and their guidance) and the clauses of the principal legislative drivers, e.g. HIPAA / SOX / GLB etc. By this means adoption of these guidelines would be facilitated, since it would provide to those implementing it a direct path to demonstrating compliance.

A consensus minimum standard of due care for protecting data on networked computers that is simple to use even by those organizations without the benefit of a full-blown security program could raise the level of protection afforded all sensitive information and at the same time lower the costs of complying with the standards. Costs would be reduced because, once the minimum standards are set, economies of scale allow vendors of information systems to provide all their thousands of customers with the tools needed to easily meet the guidelines. These guidelines would also allow organization to 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 minimum standards of due care organizations will also be better equipped to make fact based decisions when connecting information systems.

3.3. Implementation Impacts of the Proposed Technical Report

3.3.1. Development Costs

A potential draft has been underway for nearly six months and is expected to be completed before April. 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 these guidelines should lead to greater consumer confidence that their private data is being protected. That in turn will help to further accelerate the acceptance of electronic commerce, electronic government, electronic health records, and other productivity-improving and quality-of-life-improving initiatives.

3.3.3. Costs and Methods for Conformity Assessment

Because the proposed guidelines parallel the PCI standard, it is reasonable to assume the early emergence of a voluntary assessment system that parallels that used for PCI compliance, although it is not the intention of this standard to require a mandatory framework for the establishment of conformity assessment. The expectation is that organizations will use these guidelines as the initial steps for compliance to ISO/IEC 27001. However, those organizations that wish security assessments may take advantage of the fact that a large community of assessors and scanners has already been certified to measure compliance with the PCI standard. Because this document is expected to parallel the PCI standard, fully qualified PCI assessors can easily have their skills expanded to become assessors for the proposed document. Under the PCI standard, smaller organizations are currently allowed to perform self assessments while the largest organizations must use independent assessors. For PCI, quarterly vulnerability scanning by outside organizations is required whether or not they hire outside self assessment. Although this document does not require the same level of conformity assessment, a large community of auditors is available to perform internal and third-party audits. The possible testing environment may range from the use of suppliers' declarations to third party testing. Although there is no requirement for conformity assessment, there is the possibility of the establishment of voluntary assessments equivalent to those in the PCI environment. The cost of voluntary conformity assessments is not known at this time.

3.3.4. Return on Investment

Some (<http://www.cfenet.com/pdfs/2004RttN.pdf>) studies estimate an overall fraud loss equal to 6% of annual revenues. Perhaps the business insurance community could help develop ROI data as reflected in reduced premiums for implementing controls as will be defined in this checklist document.

3.4. Legal Considerations

3.4.1. Patent Assertions

There are no known patents relevant to this project. ISO copyrights, if ISO documents are quoted, need to be dealt with as appropriate. The NIST documents being considered are in the public domain.

3.4.2. Dissemination of the Technical Report

Drafts of this document will be distributed electronically. There may be distribution constraints as this document reaches different stages of development and processing within INCITS. It is desired that this document be available at minimum or no fee since the target audience is smaller organizations. There are no known IPR issues.

4. Related Standards Activities

4.1. Existing Standards

ISO/IEC 27001 “Information Security Management Systems – Requirements” is a management standard within which the provisions of the proposed PII guidelines could be implemented and managed.

ISO/IEC 17799 “Information Security Management Systems – Code of Practice” provides a high-level set of security controls and guidance. The proposed PII guidelines will provide more detailed information that is wholly consistent with 17799.

Payment Card Industry Data Security Standard, Version 1.0, December 2004.
FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

NIST SP 800-53, Recommended Security Controls for Federal Information Systems, February 2005

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004

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 NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems

FIPS 200, Minimum Security Controls for Federal Information Systems

4.3. Recommendations for Close Liaison

Close liaison is recommended with the CS1 participants in the ISO Technical Committee responsible for ISO/IEC 27001 and 17799 (JTC 1/SC 27) and the new SC27 WG1 work item on Implementation Guidance which is intended to become ISO/IEC 27003.

5. Units of Measurement used in the Project

Indicate units of measurement used in the project:

- ___ 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 project. If necessary, the goal would be to use the International System of Units (SI).