# ISO/IEC JTC 1 N 8620

2007-06-20

| | |
|---|---|
| **Document Type:** | **Proposed NP** |
| **Document Title:** | **SC 27 Proposed New Work Item on "Guidelines for cybersecurity (27032)"** |
| **Document Source:** | **SC 27 Secretariat** |
| **Reference:** | |
| **Document Status:** | **This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, we will so inform the SC 27 Secretariat and this project will be added to the SC 27 Programme of Work** |
| **Action ID:** | **VOTE** |
| **Due Date:** | **2007-09-20** |
| **No. of Pages:** | **14** |

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

# ISO/IEC JTC 1/SC27 N5722

REPLACES: N

**ISO/IEC JTC 1/SC 27**

**Information technology - Security techniques**

**Secretariat: DIN, Germany**

**DOC TYPE:** Text for NP Ballot

**TITLE:** **New Work Item Proposal on Guidelines for cybersecurity (27032)**

**SOURCE:** Secretariat JTC 1/SC27

**DATE:** 2007-06-19

**PROJECT:**

**STATUS:** In accordance with resolution 32 (contained in SC27 N5939) of the 19th SC27 Plenary meeting held in St. Petersburg, 2007-05-11/12, this document is circulated to the SC27 National Bodies for a 3-month NWI letter ballot and to JTC 1 for a concurrent review.

P-Members of SC27 are requested to submit their votes on this document via the ISO e-balloting application by **2007-09-19.**

**PLEASE NOTE:** **Attachment 1 (=SC27 N5739) to SC27 N5722 provides a preliminary draft on this NWI Proposal for a concurrent review when submitting votes on this document.**

**ACTION ID:** **LB**

**DUE DATE:** **2007-09-19**

**DISTRIBUTION:** P- and L-Members
L. Rajchel, JTC 1 Secretariat
K. Brannon, ITTF
W. Fumy, SC27 Chair
M. De Soete, SC27 Vice-Chair
E. J. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenebrg, WG-Conveners

**MEDIUM:** Livelink-server

**NO. OF PAGES:** 1 + 8 + 10 (Attachment 1 = SC27 N5739)

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.ni.din.de/sc27

## New Work Item Proposal

## NP submitting

## PROPOSAL FOR A NEW WORK ITEM

| | |
|---|---|
| Date of presentation of proposal:<br>2007-05-08 | Proposer: ISO/IEC JTC 1 SC27 |
| Secretariat: DIN, Germany | **ISO/IEC JTC 1/SC27 N5722** |

**A proposal for a new work item** shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

**Presentation of the proposal**

**Title: Guidelines for cybersecurity**

**Scope**

Cybersecurity concerns the protection of assets belonging to both organizations and users in the cyber environment. The cyber environment in this context is defined as the public on-line environment (generally the Internet) as distinct from “enterprise cyberspace” (closed internal networks specific to individual organizations or groups of organizations).

This standard will provide comprehensive guidelines on cybersecurity. It will address the issue on two levels:

1. First, it will offer ‘best practice’ guidance in achieving and maintaining security in the cyber environment for audiences in a number of categories as defined below.
2. Second, it will address the requirement for a high level of co-operation, information-sharing and joint action in tackling the technical issues involved in cybersecurity. This needs to be achieved both between individuals and organizations at a national level and internationally.

The primary audiences for the standard are:

- Cyberspace service providers such as Internet Service Providers (ISPs), web service providers, outsourcing and data back-up service providers, on-line payment bureaux, on-line commerce operators, entertainment service providers and others.
- Enterprises including not only commercial organizations but also non-profit bodies and other organizations in fields such as healthcare and education.
- Governments.

End users, while highly important, are not seen as a key target audience as they are not in general direct users of international standards.

The standard will not offer technical solutions to individual cybersecurity issues, which are already being developed by other bodies as described below.

**Purpose and justification** –

Security in the cyber environment is a subject of considerable and growing concern, not only in government and corporate environments, but also to private individuals, particularly as use of the Internet continues to spread. This is characterized by issues such as identity theft, phishing, spam, spyware, cybercrime and many others, which not only cause considerable damage at the individual incident level but also affect the efficiency and reliability of the cyber environment and undermine confidence in on-line systems. As a result much work is currently under way in a wide variety of fora to address these issues and in particular to provide technical solutions to them.

The above – and numerous other – individual technical cybersecurity issues are already being tackled by organizations such as ITU-T SG17, OECD, APEC, IETF and a number of ICT industry bodies. In many cases there is overlap and duplication between initiatives in a particular area, and there is consequently little scope for ISO/IEC JTC1 SC27 to initiate any further developments addressing technical issues in cybersecurity.

However, there are very few independent resources which provide more broadly-focussed guidance to both service providers in cyberspace and users (organizations and end users) on achieving and maintaining security in this environment.

The thrust of this standard is to address this lack and to offer an overview and guidance across the whole field of cybersecurity, in particular addressing behavioural, organizational and procedural issues. It provides reliable, up-to-date, independent and usable guidance and advice at all levels of the usage of cyberspace, from individual end users to operators of information systems and providers of a wide range of cyberspace-based services.

As such it is intended to become a widely-accepted reference which will remain relevant to its target audiences while individual technical issues arise and are dealt with by the issue-specific developments mentioned above.

**Programme of work**

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?
_X_ a single International Standard

___ more than one International Standard (expected number: ..... )
____ a multi-part International Standard consisting of ..... parts
____ an amendment or amendments to the following International Standard(s) .....
____ a technical report , type .....

And which standard development track is recommended for the approved new work item?

_X__ a. Default Timeframe

___ b. Accelerated Timeframe

____ c. Extended Timeframe

**Relevant documents to be considered**

- ITU-T SG17 document TD2313 X.cso – Overview of Cybersecurity

**Co-operation and liaison**

- ITU-T SG17
- OECD Working Party on Information Security and Protection (WPISP)
- APEC Telecommunications and Information Working Group (APEC TEL)
- Internet Engineering Task Force (IETF)

**Preparatory work offered with target date(s)**

Target dates:

| | | | | |
|---|---|---|---|---|
| **WD 2007-07-07** | **CD 2007-10-05** | **FCD 2008-04-19** | **FDIS 2008-10** | **IS 2009-02** |

**Signature:**

Will the service of a maintenance agency or registration authority be required .....No.....
- If yes, have you identified a potential candidate? .....
- If yes, indicate name .....

Are there any known requirements for coding? .....No.....
-If yes, please specify on a separate page

Does the proposed standard concern known patented items? No
- If yes, please provide full information in an annex.

**Are there any known accessibility requirements and or dependencies (see: http://www.jtc1access.org)? .....no.....**
**- If yes, please specify on a separate page**

Are there any known requirements for cultural and linguistic adaptability? .....no.....

**Comments and recommendations of the JTC 1 or SC 27**- attach a separate page as an annex, if necessary

**Comments with respect to the proposal in general, and recommendations thereon:**
It is proposed to assign this new item to JTC 1/SC 27

**Voting on the proposal** - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

| **Date of circulation:** | **Closing date for voting:** | **Signature of Secretary:** |
|---|---|---|
| 2007-06-19 | 2007-09-19 | Krystyna Passia<br>JTC 1/SC27 Secretariat |

| ***NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA*** | | |
|---|---|---|
| **Criterion** | **Validity** | **Explanation** |
| **A. Business Requirement** | | |
| A.1 Market Requirement | Essential ___<br>Desirable _X__<br>Supportive ___ | Although many different bodies are currently engaged in developing guidelines, recommendations and standards in the field of cybersecurity, in nearly every case these are of a technical nature and are generally intended to address specific individual elements (threats) – for example, spam, malware, botnets, phishing and so on.<br><br>There is a lack of generally-available, independent and comprehensive guidance for organisations and individuals on the behavioural, organisational and procedural aspects of achieving and maintaining an adequate level of security in cyberspace. In particular the requirement for co-operation, information-sharing and joint action, both between organisations and internationally, is not addressed in currently-available documents.<br><br>This standard will therefore provide a desirable complement and introduction to the more specific technical documents available from other sources. |

| | | |
|---|---|---|
| A.2 Regulatory Context | Essential ___<br>Desirable ___<br>Supportive _X__<br>Not Relevant __ | At present there is little perceived interest in regulating or legislating for cybersecurity in any context. However, the recommendations and guidelines contained in this standard will be able to be used as the basis for the development of either national, cross-border or industry-specific regulatory developments if desired or appropriate.<br><br>This standard will also be complementary to the ISMS standards ISO/IEC 27001 and 27002. |
| **B. Related Work** | | |
| B.1 Completion/Maintenance of current standards | Yes ___<br>No_X_ | |
| B.2 Commitment to other organisation | Yes ___<br>No_X_ | |
| B.3 Other Source of standards | Yes ___<br>No_X_ | |
| **C. Technical Status** | | |
| C.1 Mature Technology | Yes _X_<br>No___ | |
| C.2 Prospective Technology | Yes __<br>No_X_ | |
| C.3 Models/Tools | Yes _X_<br>No___ | |
| **D. Conformity Assessment and Interoperability** | | |
| D.1 Conformity Assessment | Yes __<br>No_X__ | |
| D.2 Interoperability | Yes __<br>No_X__ | |
| **E. Adaptability to Culture, Language, Human Functioning and Context of Use** | | |
| E1. Cultural and Linguistic Adaptability | Yes____<br>No _X_ | |

| | | |
|---|---|---|
| E.2 Adaptability to Human Functioning and Context of Use | Yes ___<br>No _X_ | |
| **F. Other Justification** | | |

**Notes to Proforma**

**A. Business Relevance.** That which identifies market place relevance in terms of what problem is being solved and or need being addressed.

A.1 Market Requirement. When submitting a NP, the proposer shall identify the nature of the Market Requirement, assessing the extent to which it is essential, desirable or merely supportive of some other project.

A.2 Technical Regulation. If a Regulatory requirement is deemed to exist - e.g. for an area of public concern e.g. Information Security, Data protection, potentially leading to regulatory/public interest action based on the use of this voluntary international standard - the proposer shall identify this here.

**B. Related Work.** Aspects of the relationship of this NP to other areas of standardisation work shall be identified in this section.

B.1 Competition/Maintenance. If this NP is concerned with completing or maintaining existing standards, those concerned shall be identified here.

B.2 External Commitment. Groups, bodies, or for a external to JTC 1 to which a commitment has been made by JTC for Co-operation and or collaboration on this NP shall be identified here.

B.3 External Std/Specification. If other activities creating standards or specifications in this topic area are known to exist or be planned, and which might be available to JTC 1 as PAS, they shall be identified here.

**C. Technical Status.** The proposer shall indicate here an assessment of the extent to which the proposed standard is supported by current technology.

C.1 Mature Technology. Indicate here the extent to which the technology is reasonably stable and ripe for standardisation.

C.2 Prospective Technology. If the NP is anticipatory in nature based on expected or forecasted need, this shall be indicated here.

C.3 Models/Tools. If the NP relates to the creation of supportive reference models or tools, this shall be indicated here.

**D. Conformity Assessment and Interoperability**

D.1 Indicate here if Conformity Assessment is relevant to your project. If so, indicate how it is addressed in your project plan.

D.2 Indicate here if Interoperability is relevant to your project. If so, indicate how it is addressed in your project plan

**E. Adaptability to Culture, Language, Human Functioning and Context of Use**

NOTE: The following criteria do not mandate any feature for adaptability to culture, language, human functioning or context of use. The following criteria require that if any features are provided for adapting to culture, language, human functioning or context of use by the new Work Item proposal, then the proposer is required to identify these features.

E.1 Cultural and Linguistic Adaptability. Indicate here if cultural and natural language adaptability is applicable to your project. If so, indicate how it is addressed in your project

plan. ISO/IEC TR 19764 (Guidelines, methodology, and reference criteria for cultural and linguistic adaptability in information technology products) now defines it in a simplified way:

“ability for a product, while keeping its portability and interoperability properties, to:

- be internationalized, that is, be adapted to the special characteristics of natural languages and the commonly accepted rules for their se, or of cultures in a given geographical region;

- take into account the usual needs of any category of users, with the exception of specific needs related to physical constraints”

*Examples of characteristics of natural languages are: national characters and associated elements (such as hyphens, dashes, and punctuation marks), writing systems, correct transformation of characters, dates and measures, sorting and searching rules, coding of national entities (such as country and currency codes), presentation of telephone numbers and keyboard layouts. Related terms are localization, jurisdiction and multilingualism.*

E.2 Adaptability to Human Functioning and Context of Use. Indicate here whether the proposed standard takes into account diverse human functioning and diverse contexts of use. If so, indicate how it is addressed in your project plan.

NOTE:

1. Human functioning is defined by the World Health Organization at **http://www3.who.int/icf/beginners/bg.pdf as:**
   <<In ICF (International Classification of Functioning, Disability and Health), the term functioning refers to all body functions, activities and participation.>>

2. 2. Content of use is defined in ISO 9241-11:1998 (Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability) as: <<Users, tasks, equipment (hardware, software and materials), and the physical and societal environments in which a product is used.>>

3. 3. Guidance for Standard Developers to address the needs of older persons and persons with disabilities).

**F. Other Justification** Any other aspects of background information justifying this NP shall be indicated here

**PROPOSAL FOR A NEW WORK ITEM**

| Date of presentation of proposal:<br><br>2004-01-07 | Proposer:<br>US National Body |
|---|---|
| Secretariat:<br>ANSI | ISO/IEC JTC 1/SC 22 N **3704** |

A **proposal for a new work item** shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

**Presentation of the proposal** - to be completed by the proposer Guidelines for proposing and justifying a new work item are given in ISO Guide 26.

**Title**

Specification for secure C Library functions.

**Scope**

To introduce a redefinition of current C library functions -- including new library functions, macros, and types -- to the C programming Language to make them secure and safe in today's programming environment. These functions will attempt to eliminate buffer overflow, will have advanced error reporting, will in some cases contain parameter validation, and will have other features that are needed in today's programming environment to help guarantee more secure and safe programs.

**Purpose and justification**

The programming language C as specified by the International Standard ISO/IEC 9899:1999 provides little in the way of secure library functions. Security has quickly become one of the most important issues in programming, and the C programming language must stay abreast of this requirement. The only way to accomplish this is to add secure functionality to the C Programming language library.

This NP proposes to establish a new project to produce a Technical Report (type 2) in which existing Standard C Library functions and macros are redefined (renamed) to take into account buffer overrun, more robust error reporting, parameter validation, and any other feature that is required to make the functions and macros secure. In some cases there will no doubt need to be new functions, macros and types defined. Some other issues (like callback, thread safety, reentry safety) will be studied; it is not yet clear whether this functionality is suitable for specification in the proposed Technical Report, or if the topics will be dealt with in a future Technical Report (under another NP).

The main focus of this project will be to redefine the C library functions that have been identified as unsafe or non-secure in today's programming environment. Any and all prior art will be taken into account while developing the specifications for the redefinition of a secure and safe C Library.

The project also includes the production of the text for a Rationale document (either separate or as part of the project document).

**Programme of work**

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?
____ a single International Standard more than one International Standard (expected number: ..... )
____ a multi-part International Standard consisting of ..... parts
____ an amendment or amendments to the following International Standard(s) .....
_X__ a technical report , type 2

**Relevant documents to be considered**

- ISO/IEC 9899:1999 - Programming Language C

- ISO/IEC JTC 1/SC22 WG14 N1007 - Security and Standard C Libraries
- ISO/IEC JTC 1/SC22 WG14 N1031 - Specification for secure C Libray functions
- ISO/IEC 11404:1996 - Language-independent datatypes.

**Cooperation and liaison**

All ISO/IEC JTC 1/SC22 Working groups that have an interest in supporting many natural languages, especially ISO/IEC JTC 1/SC22 WG21 (C++).

**Preparatory work offered with target date(s)**

A PDTR document will be ready for registration 24 months after the approval of the project by JTC 1.

**Signature:**

for
ANSI
P-Member of JTC 1/SC 22

Will the service of a maintenance agency or registration authority be required? .....NO.....
- If yes, have you identified a potential candidate? .....
- If yes, indicate name .....

Are there any known requirements for coding? .....NO.....
-If yes, please specify on a separate page

Are there any known requirements for cultural and linguistic adaptability? .....NO....
- If yes, please specify on a separate page

Does the proposed standard concern known patented items? .....NO.....
- If yes, please provide full information in an annex

**Comments and recommendations of the JTC 1 Secretariat - attach a separate page as an annex, if necessary**

**Comments with respect to the proposal in general, and recommendations thereon:**
It is proposed to assign this new item to JTC 1/SC22 WG14
The proposed project editor is Randy Meyers (rmeyers@ix.netcom.com) of the United States, the proposed backup project editor is P. J. Plauger (pjp@dinkumware.com) of the United States. Both are members in good standing of NCITS J11.

**Voting on the proposal - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).**

| **Date of circulation:** | **Closing date for voting:** | **Signature of JTC 1/SC 22 Secretary:** |
|---|---|---|
| 2004-01-09 | 2004-04-09 | Matt Deane |

---

| ***NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA*** | | |
|---|---|---|
| **Criterion** | **Validity** | **Explanation** |
| **A Business Requirement** | | |
| A.1 Market Requirement | Essential ___<br>Desirable ___ | |

| | | |
|---|---|---|
| | Supportive ___ | |
| A.2 Regulatory Context | Essential ___<br>Desirable ___<br>Supportive ___<br>Not Relevant ___ | |
| **B. Related Work** | | |
| B.1 Completion/Maintence of current standards | Yes ___<br>No___ | |
| B.2 Commitment to other organization | Yes ___<br>No___ | |
| B.3 Other Source of standards | Yes ___<br>No___ | |
| **C. Technical Status** | | |
| C.1 Mature Technology | Yes ___<br>No___ | |
| C.2 Prospective Technology | Yes ___<br>No___ | |
| C.3 Models/Tools | Yes ___<br>No___ | |
| **D. Conformity Assessment and Interoperability** | | |
| D.1 Conformity Assessment | Yes ___<br>No___ | |
| D.2 Interoperability | Yes ___<br>No___ | |
| **E. Other Justification** | | |

---

**Notes to Proforma**

**A. Business Relevance. That which identifies market place relevance in terms of what problem is being solved and or need being addressed.**

**A.1. Market Requirement. When submitting a NP, the proposer shall identify the nature of the Market Requirement, assessing the extent to which it is essential, desirable or merely supportive of some other project.**

**A.2 Technical Regulation. If a Regulatory requirement is deemed to exist - e.g. for an area of public concern e.g. Information Security, Data protection, potentially leading to regulatory/public interest action based on the use of this voluntary international standard - the proposer shall identify this here.**

**B. Related Work. Aspects of the relationship of this NP to other areas of standardization work shall be identified in this section.**

**B.1 Competition/Maintenance. If this NP is concerned with completing or maintaining existing standards, those concerned shall be identified here.**

**B.2 External Commitment. Groups, bodies, or fora external to JTC1 to which a commitment has been made by JTC for cooperation and or collaboration on this NP shall be identified here.**

**B.3 External Std/Specification. If other activities creating standards or specifications in this topic area are known to exist or be planned, and which might be available to JTC1 as PAS, they shall be identified here.**

**C. Technical Status. The proposer shall indicate here an assessment of the extent to which the proposed standard is supported by current technology.**

**C.1 Mature Technology. Indicate here the extent to which the technology is reasonably stable and ripe for standardization.**

**C.2 Prospective Technology. If the NP is anticipatory in nature based on expected or forecasted need, this shall be indicated here.**

**C.3 Models/Tools. If the NP relates to the creation of supportive reference models or tools, this shall be indicated here.**

**D. Any other aspects of background information justifying this NP shall be indicated here.**

**D. Conformity Assessment and Interoperability**

**D.1 Indicate here if Conformity Assessment is relevant to your project. If so, indicate how it is addressed in your project plan.**

**D.2 Indicate here if Interoperability is relevant to your project. If so, indicate how it is addressed in your project plan.**