ISO/IEC JTC 1
Information Technology

Document Type: information from ISO CS

Document Title: Security related standardization - follow-up on the ISO/TMB AGS1 recommendations

Document Source: ISO/CS

Document Status: This document is circulated to JTC 1 National Bodies for review and consideration at the November 2008 JTC 1 Plenary meeting in Nara.

Action ID: ACT

Due Date:

No. of Pages: 13

Organisation internationale de normalisation
International Organization for Standardization
Международная Организация по Стандартизации

**TO THE SECRETARIES OF THE ISO TCS AND
ISO/IEC JTC 1 SCS <u>CONCERNED</u>**

Your ref.
Our ref.

Date   2008-10-16

Security related standardization - follow-up on the ISO/TMB AGS[1] recommendations

Dear Sir or Madam,

At its meeting in January 2004, the ISO Technical Management Board approved the formation of a high-level strategic Advisory Group on Security (AGS) to

- conduct a review of existing ISO deliverables related to the field of security, which may include (but is not limited to) the subjects of:

    1)   Training programmes and equipment for responders.

    2)   Private sector emergency preparedness and business continuity.

    3)   Identification techniques, including biometrics.

    4)   Emergency communications.

    5)   Inter-modal supply chain security.

    6)   Risk assessment.

    7)   Biological and chemical threat agents.

    8)   Cyber security.

    9)   Civil defence.

- assess the needs of all relevant stakeholders for international security standards.

- assess relevant standards developed by other organizations that may support international needs for security standards.

- recommend actions to be taken by the ISO Council and/or ISO/TMB on subjects within the field of security that may benefit from the development of international standards and that ISO would have the capability to provide.

---

[1] Advisory Group Security

Following two meetings of the AGS, a report was submitted to the TMB in January 2005 and was discussed by the TMB at a meeting held on 10-11 February 2005. Among the resolutions taken at this meeting were the following:

> **Technical Management Board resolution 4/2005**
> **Security (1)**
> The Technical Management Board
> <u>thanks</u> the chair, Dr. George Arnold, and members of the Advisory Group on Security for their excellent report,
> <u>agrees</u> that the report be made available to all ISO member bodies,
> <u>accepts</u> recommendation 1 to establish a permanent group to oversee and coordinate standardization activities relevant to security, and invites Dr. Arnold to chair the group,
> <u>invites</u> IEC to consider whether they would be willing to make this a joint ISO/IEC group,
> <u>notes</u> the current ISO Council discussion on natural disasters and that this may have consequences for the proposed group,
> <u>asks</u> ISO/CS staff to work with IEC staff if appropriate to develop proposals for the terms of reference and membership of the proposed group, which shall continue to be a Strategic Advisory Group.
>
> **Technical Management Board resolution 11/2005**
> **Security (8)**
> The Technical Management Board,
> <u>refers</u> AGS recommendations 9 to 15 to the relevant ISO (ISO/IEC) committees and requests them to provide feedback on proposed follow-up actions.

The group, established in accordance with resolution 4/2005 has in the meantime been transformed into an ISO/IEC/ITU-T joint strategic advisory group and over the last few years has provided input to ISO/TC 223, been developing a guide on the inclusion of security aspects in standards, and has organised a number of workshops e.g. on Transit Security. It has, however, now requested that the ISO committees addressed in AGS recommendations 9 to 15 (see annex) provide feedback on follow-up before 15 December for consideration at the next meeting in January 2009.

Thanking you in advance.

Yours sincerely,

Secretariat SAG-S

Enclosures

ISO Advisory Group on Security Recommendations

9. Protection for first responders

ISO/TC94, which develops standards for protective clothing and equipment, should expand its work programme to specifically address new technologies for protective clothing for first responders, ensuring the scope of any new projects accounts for the differences in physical attributes.

10. Equipment for first responders

There is great interest in standards for equipment that first responders use to detect chemical, biological, explosives or radiological threats. It would be beneficial for such standards to exist at the international level. Relevant ISO TCs (see Annex B) should consider national standards or other specifications that can be fast-tracked through ISO, for example the IEEE standards (ANSI N 42.32 through N 42.35 on radiological and nuclear detection).

11. Personal identification

Given this is an extremely important area and is actively covered by ISO/IEC JTC1 SCs 17, 27, and 37, the AGS recommends continuing focus and collaboration of the subcommittees, as well as, if possible, acceleration of this work.

12. Cybersecurity

The AGS recommends that JTC 1/SC 27 examine whether standards or guidelines could play a role in preventing new types of attack, such as viruses, worms, and phishing. The AGS noting that ISO/IEC JTC 1/SC 27 has been very active in providing general guidelines and deliverables in response to cyber security threats, recommends that ISO/IEC JTC 1/SC 27 review ongoing work in other Fora with the view to covering any gaps in this area by the transferring of existing best practices into ISO deliverables. For information an overview of ongoing cyber security initiatives and potential "gap" areas is shown in Annex C.

13. Healthcare

The AGS recommends that ISO/TC 198, which deals with sterilization of health care products, examine the possibility to expand its work to include subjects such as infection control, sterilization, and contamination units.

14. Resources

The AGS recommends that ISO/TC 224 (water quality), ISO/TC 34 (food products) and ISO/TC 146 (air quality) (see scopes in Annex B) examine security aspects such as standards for detection and protection against threats of contamination. Also in the area of Natural Gas (critical infrastructure) all related TCs should review their work programmes with a view to addressing the potential for deliverables on security.

15. Transportation systems

Aircraft, trains, buses, trucks, and ships are extremely vulnerable to attack and pose a high risk to security. They represent both targets with the potential for mass

casualties, as well as weapons that can be used to destroy infrastructure and inflict mass casualties.

- In the area of ships, ISO already has an active work program underway in ISO/TC8 on marine technology, which includes the security aspects of ships and marine ports.

However, ISO's contributions to the security of other means of transportation are more limited.

- In the area of air transport security, ICAO and IATA are the principal international organizations responsible for the adoption of civil aviation standards. Security standards produced by these organizations currently reference ISO standards for identity cards, biometrics, and IT systems. The AGS recommends that ISO/TC 20, which deals with aircraft and related ground support systems, consult with ICAO and IATA to determine whether there are additional areas to which ISO should contribute.

- ISO does not have a TC concerned with rail transportation, although ISO/TC204 on intelligent transportation systems does cover information aspects of ground transportation including rail. There is the potential for ISO to make standards contributions in the area of identity, security screening systems, security management, and new technologies to protect against attack such as optical or infrared systems to monitor tracks. We recommend that ISO engage in dialog with the relevant inter-governmental agency, UIC, to determine whether an ISO role would be helpful.

- ISO has significant work related to road transport. Certain aspects of security are being addressed in ISO's work. For example, ISO/TC 204 provides a focus for information-related aspects of security, ISO/TC 104 deals with electronic and mechanical seals on freight containers, and ISO/IEC JTC 1/SC 31 deals with application of technologies such as RFID, which can enhance security. Broader contributions may be possible to introduce standards that enhance physical security, make hijacking or theft more difficult, or provide security management systems and risk assessment tools. The AGS recommends that ISO consult with relevant inter-governmental agencies such as UN/ECE, as well as key industry players to determine whether there are opportunities for ISO to contribute in these areas. Also that TC 204 establish liaison with ISO/IEC JTC 1/SC 17 and 27 to ensure the requirements for identity and security in general are being addressed

Annex B

TCs involved in security

The following is a list of ISO and ISO/IEC Technical Committees, and subcommittees with their scopes that have been identified as having security related projects.

JTC 1/SC 17 : Cards and personal identification

Scope:
Standardization in the area of
a) identification and related documents,
b) cards,
and devices associated with their use in interindustry applications and international interchange.

JTC 1/SC 27 : IT Security techniques

Scope:
Standardization of generic methods and techniques for IT security. This includes:
-identification of generic requirements (including requirements methodology) for IT system security services;
-development of security techniques and mechanisms (including registration procedures and relationships of security components);
-development of security guidelines (e.g., interpretative documents, risk analysis); and
-development of management support documentation and standards (e.g. terminology and security evaluation criteria)

JTC 1/SC 31 : Automatic identification and data capture techniques

Scope:
Standardization of data formats, data syntax, data structures, data encoding and technologies for the process of automatic identification and data capture.

JTC 1/SC 37 : Biometrics

Scope:
Standardization of genetic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.

TC 8 : Ships and marine technology

Scope:
Standardization of design, construction, structural elements, outfitting parts, equipment,

methods and technology, and marine environmental matters, used in shipbuilding and the operation of ships, comprising sea-going ships, vessels for inland navigation, offshore structures, ship-to-shore interface and all other marine structures subject to IMO requirements.

TC 20 : Aircraft and space vehicles

Scope:
Standardization of materials, components and equipment for construction and operation of aircraft and space vehicles as well as equipment used in the servicing and maintenance of these vehicles.

TC 21 : Equipment for fire protection and fire fighting

Scope:
Standardization in the field of all fire protection and fire fighting apparatus and equipment including extinguishing media as well as the personal equipment of the fire fighter, and related work on terminology, classification and symbols.
Approval of advisory documents relating to the general principles and application of equipment and apparatus for fire protection and fire fighting.

TC 22 : Road vehicles

Scope:
All questions of standardization concerning compatibility, interchangeability and safety, with particular reference to terminology and test procedures (including the characteristics of instrumentation) for evaluating the performance of the following types of road vehicles and their equipment as defined in the relevant items of Article 1 of the convention on Road Traffic, Vienna in 1968 concluded under the auspices of the United Nations:

- mopeds (item m);
- motor cycles (item n);
- motor vehicles (item p);
- trailers (item q);
- semi-trailers (item r);
- light trailers (item s);
- combination vehicles (item t);
- articulated vehicles (item u).

TC 28 : Petroleum products and lubricants

Scope:
Standardization of methods of measurement, sampling and test, terminology, classifications and specifications for petroleum, petroleum products and non-petroleum based lubricants and hydraulic fluids.

TC 34 : Food products

Scope:
Standardization in the field of human and animal foodstuffs as well as animal and vegetable

propagation materials, in particular terminology, sampling, methods of test and analysis, product specifications and requirements for packaging, storage and transportation.

TC 58 : Gas cylinders

Scope:
Standardization of gas cylinders, their fittings and characteristics relating to their manufacture and use.

TC 67 : Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries

Scope:
Standardization of the materials, equipment and offshore structures used in the drilling, production, transport by pipelines and processing of liquid and gaseous hydrocarbons within the petroleum, petrochemical and natural gas industries.

TC 68/SC 2 : Security management and general banking operations

Scope:
Standardization for information security management and operations in financial services, excluding
- security and operations in retail financial services (SC6), and
- operations in securities and related financial instruments (SC4).

TC 68/SC 6 : Retail financial services

Scope:
Standardisation in the field of retail financial services, including cards, related media and operations.

The scope covers content, usage, interchange and security of retail applications.

TC 76 : Transfusion, infusion and injection equipment for medical and pharmaceutical use

Scope:
Standardization of transfusion, infusion and injection equipment for medical and pharmaceutical use; terms and definitions for such equipment; specifications for quality and performance of materials and components.

Standardization of containers (such as infusion bottles, injection vials, ampoules, glass cylinders, cartridges, prefillable syringes, etc.) and devices (such as giving sets, blood collecting tubes, etc.) as well as pertinent primary and secondary packaging and functional components (such as elastomeric closures, caps, pipettes and accessories) for medical and pharmaceutical use.

TC 85 : Nuclear energy

Scope:
Standardization in the field of peaceful applications of nuclear energy and of the protection of individuals against all sources of ionising radiations.

TC 92 : Fire safety

Scope:
Standardization of the methods of assessing

- fire hazards and fire risk to life and to property;
- the contribution of design, materials, building materials, products and components to fire safety

and methods of mitigating the fire hazards and fire risks by determining the performance and behaviour of these materials, products and components, as well as of buildings and structures.

TC 94 : Personal safety -- Protective clothing and equipment

Scope:
Standardization of the quality and performance of clothing and personal equipment designed to safeguard persons against hazards other than those concerned with nuclear radiation.

TC 98 : Bases for design of structures

Scope:
Standardization of the bases for design of structures irrespective of the material of construction including especially terminology and symbols, load, forces and other actions and limitations of deformations. Consideration and coordination of basic reliability requirements concerning the structures as a whole, including consideration of structures made of particular materials (steel, stone, concrete, wood, etc.) as far as is necessary for the preparation of a common approach to reliability in liaison with the relevant technical committees.

TC 104 : Freight containers

Scope:
Standardization of freight containers, having an external volume of one cubic meter (35.3 cubic feet) and greater, as regards terminology, classification, dimensions, specifications, handling, test methods and marking.

TC 122 : Packaging

Scope:
Standardization in the field of packaging with regard to terminology and definitions, packaging dimensions, performance requirements and tests.

TC 145 : Graphical symbols

Scope:
Standardization in the field of graphical symbols as well as of colours and shapes, whenever these elements form part of the message that a symbol is intended to convey, e.g. a safety sign.

Establishing principles for preparation, coordination and application of graphical symbols. General responsibility for the review and the coordination of those already existing, those under study, and those to be established. The standardization of new graphical symbols, when requested by a technical committee, or where it does not fall within the activity of an existing technical committee.

TC 146 : Air quality

Scope:
Standardization in the field of air quality, including definitions of terms, sampling of air, measurement and reporting of air characteristics.

TC 147 : Water quality

Scope:
Standardization in the field of water quality, including definition of terms, sampling of waters, measurement and reporting of water characteristics.

TC 154 : Processes, data elements and documents in commerce, industry and administration

Scope:
International standardization and registration of business, and administration processes and supporting data used for information interchange between and within individual organizations and support for standardization activities in the field of industrial data.
Development and maintenance of application specific meta standards for:

- process specification (in the absence of development by other technical committees);
- data specification with content;
- forms-layout (paper / electronic).

Development and maintenance of standards for

- process identification (in the absence of development by other technical committees);

- data identification.

Maintenance of the EDIFACT-Syntax.

TC 159 : Ergonomics

Scope:
Standardization in the field of ergonomics, including terminology, methodology, and human factors data.

TC 162 : Doors and windows

Scope:
Standardization in the field of doors, doorsets and windows including hardware, manufactured from any suitable material covering the specific performance requirements, terminology, manufacturing sizes and dimensions, and methods of test.

TC 184 : Industrial automation systems and integration

Scope:
Standardization in the field of industrial automation and integration concerning discrete part manufacturing and encompassing the application of multiple technologies, i.e. information systems, machines and equipment, and telecommunications.

TC 190 : Soil quality

Scope:
Standardization in the field of soil quality, including classification, definition of terms, sampling of soils, measurement and reporting of soil characteristics.

TC 192 : Gas turbines

Scope:
Standardization in the field of all aspects of gas turbine design, application, installation, operation and maintenance, including simple turbine cycles, combined cycle systems, definitions, procurement, acceptance, performance, environment (on the gas turbine itself and the external environment) and methods of test.
ISO / TC 192 is responsible for preparing horizontal standards for all types of gas turbines. Work on aero gas turbine engines shall be undertaken in liaison with those technique committees having the primary responsibility.

TC 197 : Hydrogen technologies

Scope:
Standardization in the field of systems and devices for the production, storage, transport, measurement and use of hydrogen.

TC 204 : Intelligent transport systems

Scope:
Standardization of information, communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveller information, traffic management, public transport, commercial transport, emergency services and commercial services in the intelligent transport systems (ITS) field.

TC 211 : Geographic information/Geomatics

Scope:
Standardization in the field of digital geographic information. *Note:* This work aims to establish a structured set of standards for information concerning objects or phenomena that are directly or indirectly associated with a location relative to the Earth.

These standards may specify, for geographic information, methods, tools and services for data management (including definition and description), acquiring, processing, analyzing, accessing, presenting and transferring such data in digital / electronic form between different users, systems and locations.

The work shall link to appropriate standards for information technology and data where possible, and provide a framework for the development of sector-specific applications using geographic data.

TC 212 : Clinical laboratory testing and in vitro diagnostic test systems

Scope:
Standardization and guidance in the field of laboratory medicine and in vitro diagnostic test systems. This includes, for example, quality management, pre- and post-analytical procedures, analytical performance, laboratory safety, reference systems and quality assurance.

TC 215 : Health informatics

Scope:
Standardization in the field of information for health, and Health Information and Communications Technology (ICT) to achieve compatibility and interoperability between independent systems. Also, to ensure compatibility of data for comparative statistical purposes (e.g. classifications), and to reduce duplication of effort and redundancies.

TC 220 : Cryogenic vessels

Scope:
Standardization in the field of insulated vessels (vacuum or non-vacuum) for the storage and the transport of refrigerated liquefied gases of class 2 of "Recommendations on the Transport of Dangerous Goods - Model regulations - of the United Nations", in particular concerning the design of the vessels and their safety accessories, gas / materials

compatibility, insulation performance, the operational requirements of the equipment and accessories.

TC 223 : Civil defence

Scope:
Standardization in the field of civil defence (protection); monitoring and prediction of emergency situations of natural and technogenic character; elimination of consequence from natural disasters, emergencies and catastrophes; tools, equipment and outfit for human salvation; public safety systems, training and education of population.

TC 224 : Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators

Scope:
Standardization of a framework for the definition and measurement of service activities relating to drinking water supply systems and wastewater systems.

The standardization includes the definition of a language common to the different stakeholders, the definition of the characteristics of the elements of the service according to the consumers expectations, a list of requirements to fulfil for the management of a drinking water supply system and a wastewater system, service quality criteria and a related system of performance indicators, without setting any target values or thresholds.