



Document : **ISO/IEC/TMB SAG N05**

Date : 2005-10-25

TITLE : Final Report of ISO Advisory Group on Security

SOURCE : ISO/IEC/TMB SAG-Security Secretariat

REQUESTED ACTION : Review for Agenda item 4 of the SAG meeting, 29-30 November 2005, Geneva

DISTRIBUTION : ISO/IEC/TMB SAG-Security members



Document : **ISO/TMB AGS N 46**

Date : 2005-01-06

TITLE : Final Report of ISO Advisory Group on Security

SOURCE : ISO/TMB AG-Security Secretariat

REQUESTED ACTION : For information

DISTRIBUTION : ISO/TMB AG-Security members

CONTENTS

- 1 Summary
- 2 Background
- 3 Scope, definitions and terms
- 4 Security model
- 5 Stakeholders needs
- 6 Surveys of existing work of ISO, ITU-T and IEC
- 7 General assessment
- 8 Recommendations
- 9 Concluding observations

ANNEXES

ISO Advisory Group on Security final report

1 Summary

Acts of terrorism have become a global problem that claims thousands of lives every year. Ensuring the security of citizens has gone from something we take for granted to one of the most important priorities for societies around the world. In the aftermath of the September 11, 2001 attacks in the United States, several studies concluded that standards play a critical role in ensuring security, and that in key areas standards were either lacking or new standards were needed.

Recognizing the global nature of security concerns, in January 2004 the ISO Council directed the Technical Management Board to form a high-level strategic Advisory Group on Security (AGS). The AGS was tasked to review ISO and other organizations' existing work related to security, assess the needs of relevant stakeholders, and recommend what additional standards work should be undertaken to support international standardization needs related to security. Representatives of eight countries were named to the AGS. It held its first meeting on June 1, 2004 and was asked to make its recommendations to the TMB by December 31, 2004.

The AGS noted that security is not limited to combating terrorism. The same means used to prevent or respond to terrorist events may be applied to natural or accidental disasters or cyber attacks. The AGS considered security to mean "the safety of a state, organization or individual and protection against threats such as criminal activity, terrorism, attack, or natural disaster." The AGS considered security standards in this broad context.

Following is a summary of the AGS's key recommendations :

1. **Strategic Focus.** Presently, ISO's work on security results almost entirely from "bottom-up" efforts by its Technical Committees. This needs to be supplemented with a more strategic, top-down perspective. TMB should establish a permanent Steering Committee on Security (SCS) to provide continuing strategic direction and coordination and to provide oversight for a number of new deliverables noted below.
2. **Guidelines for Technical Committees.** Security considerations must become an integral element in the products, systems and operations supporting the day-to-day functioning of society. Accordingly, consideration of security concerns must become an integral part of ISO's process for developing standards. A joint ISO/IEC working group should be established to develop a guide to provide direction to Technical Committees on when to incorporate security considerations into their work and what must be considered. SCS should provide oversight for the working group established to develop this guide. A recommended outline of the content of the guide is included in this report (see Annex A).
3. **Security Management Standards.** ISO should undertake the development of a Security Management System framework standard. This guidance document should provide the common vocabulary, concepts, and principles that underlie an effective system for managing security. It should provide a framework under which sector-specific standards, such as ISO/IEC 17799 for Information Technology, and similar deliverables in other sectors, can be integrated in a cohesive approach to managing security. SCS should provide oversight for the development of the Security Management System Framework Standard. We note that the TMB has established

an advisory group to recommend how ISO should organize its management system standards going forward, and that group may recommend an alternative approach.

4. **Security Standards Web Portal.** Many stakeholders indicated that they lack knowledge of what security standards exist and how to obtain them. ISO should establish a web page that provides a portal to ISO security standards and links to those of other organizations, as well as a roadmap and searchable index to ISO's security deliverables. SCS should provide oversight for the portal.
5. **Role of ISO/TC 223.** The AGS is concerned about the dormant status of ISO/TC 223 on Civil Defense, whose broad terms of reference include many key aspects of emergency preparedness and response. The AGS notes positively the Secretariat (GOST-R)'s intention to call a first meeting in 2005 and invite contributions on work program, structure, etc. We recommend that the TMB closely track the progress of ISO/TC 223 to ensure a successful start-up.
6. **Emergency Preparedness Standard.** Many stakeholders saw an urgent need for a standard on emergency preparedness. It is recommended that ISO develop an International Workshop Agreement (IWA) on this subject in early 2005, building upon existing national or regional standards such as ANSI/NFPA 1600, UK Civil Contingencies Secretariat Disaster Guides, and others. Once developed, this IWA deliverable should be fed into ISO/TC 223 for further progression as an International Standard.
7. **Updated and/or New Standards.** The AGS identified a number of areas in ISO's portfolio where existing standards need to be updated to address current security concerns, or where security-related standards were lacking and may need to be developed. Following are a few examples noted by the AGS:
 - a. **Built Infrastructure Protection.** The AGS notes that ISO TAG 8 coordinates work across ISO/TCs 59, 92, 162 and 145 which provide standards related to buildings. Many of the standards date to the 1980's. The AGS recommends that standards for design of buildings be reviewed and updated to make use of the studies done by NIST on the World Trade Center disaster, the applicability of new technologies for rescue from high buildings, etc.
 - b. **Protection for first responders.** ISO/TC94, which develops standards for protective clothing and equipment, should expand its work to specifically address new technologies for protective clothing for first responders.
 - c. **Equipment for first responders.** There is great interest in standards for equipment that first responders use to detect chemical, explosives, biological 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 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).
 - d. **Personal identification.** 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 if possible acceleration of this work.
 - e. **Cybersecurity.** The AGS recommends that JTC 1 examine whether standards could play a role in preventing new types of attack, such as viruses, worms, and phishing.
 - f. **Healthcare.** The AGS recommends that ISO/TC 198, which deals with sterilization of health care products, expand its work to include subjects such as infection control, sterilization, and contamination units.

- g. **Resources.** The AGS recommends that ISO/TC 224 (water systems), ISO/TC 34 (food products) and TC 146 (air quality) examine security aspects such as standards for detection and protection against threats of contamination.
- h. **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 development of 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 Technical Committee 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/TC 122 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.

2 Background

Council, at its meeting in Buenos Aires, recognized that, as a result of events in recent years, the subject of security is high on the list of government priorities as well as being of concern to the general public. It accordingly asked the Secretary-General to engage contacts with relevant international organizations and ISO members and to make an inventory/analysis of all existing security-related ISO standards, with a view to assessing further the needs for International Standards for security and the potential for additional ISO involvement. It additionally asked the Secretary-General to refer to the TMB the comments received from Council members as well as the results of the above action, for consideration of their impact on ISO's technical work. Finally it requested that a progress report be submitted for Council's meeting in March 2004.

As follow up to this resolution, the TMB Secretary had a number of contacts with ANSI (USA) concerning its activities in support of the US Department of Homeland Security and also participated in a number of meetings on security organized in Geneva. One immediate finding was the area of security has a whole range of facets and that there are many initiatives being pursued at the present time. Many of these initiatives are being pursued at the national level although there are also some groups addressing security issues under the aegis of G8. The most actively engaged international organizations at this time seem to be all involved in the multi-modal supply chain.

As a result of the complexity of the subject, it was suggested that the TMB probably needed advice from experts having an overview of the whole field of security and it was consequently proposed that the TMB establish a high-level steering committee for the field of security. Such a group of experts would be able to provide advice on the different aspects of security that needed to be addressed and current initiatives that are relevant.

In response to this the ISO Technical Management Board, at its January 2004 meeting, approved the formation of a high-level strategic Advisory Group on Security 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
 - Training programmes and equipment for responders.
 - Private sector emergency preparedness and business continuity.
 - Identification techniques, including biometrics.
 - Emergency communications.
 - Inter-modal supply chain security.
 - Risk assessment.
 - Biological and chemical threat agents.
 - Cyber security.
 - 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.

- Submit a final report to the ISO/TMB and ISO Council by 31 December 2004.

The AGS has met twice and had numerous teleconferences and has carried out the tasks of

- reaching out to stake-holders at national and international level through a survey of security needs,
- identifying what standards already exist by conducting an extensive inventory of existing deliverables and work projects in ISO technical committees as well as in ITU and IEC,

It agreed to provide its final report and recommendations to the TMB by December 31 2004.

3 Scope, definitions and terms

Scope

The Advisory Group on Security was mandated to review all aspects of security within a broad and comprehensive spectrum. The AGS view of security encompasses public safety and security, while addressing the need to design measures to ensure public safety and security that enhance, and do not impede or infringe on individual rights and freedoms.

Definitions

Security: The provision of protection against threats to people, physical assets, infrastructure, information and information technology assets including electronic networks and facilities, and to the movement of people and goods and related facilities.

Security provides safety and facilitates business commerce and trade through the safe movement of people, goods and services. At the same time, by protecting people, business and government, security enhances freedom and protects individual rights, including the right to privacy.

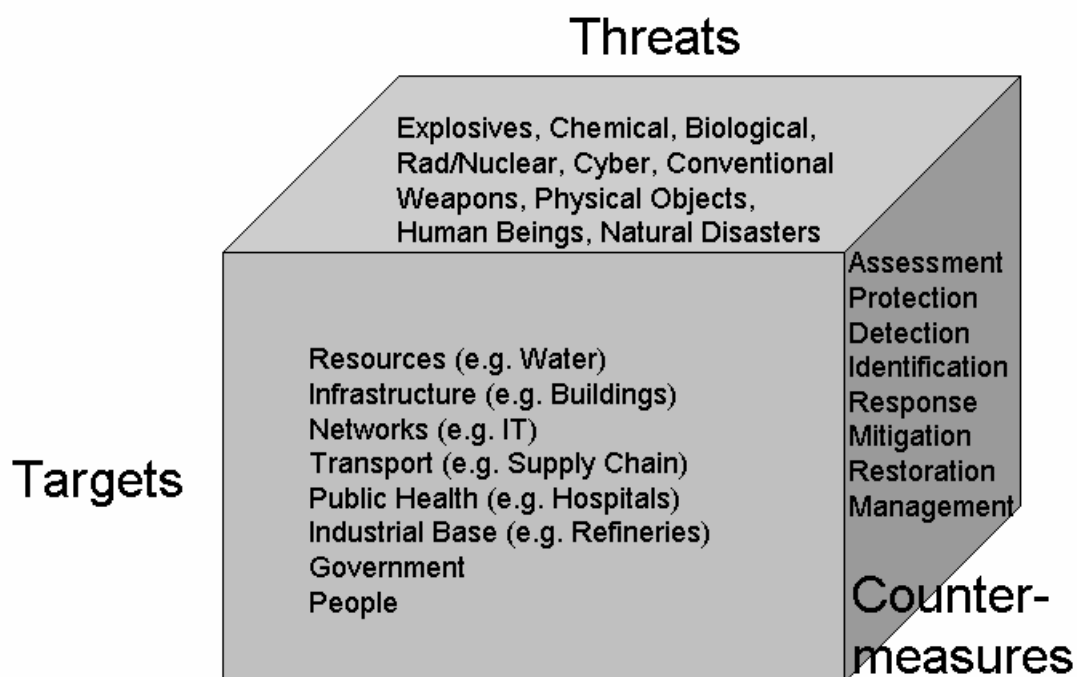
All other definitions should be extracted from existing sources, notably ISO Guide 73 on risk management, and ISO/IEC 2382 IT Terminology, and especially Part 8: Security.

The terms and definitions will be brought forward by the various committees involved to the Steering Committee on Security for decision.

It is particularly important to note that privacy, and individual rights and freedoms, are addressed within the lexicon on security.

4 Security model

The AGS took a systematic approach to identifying potential needs for security standards, existing standards, and gaps, using a security model. The model provides a framework to classify aspects of security in three dimensions: **targets, threats, and countermeasures**. The model is illustrated in the figure.



Figure

Targets are the entities, including people, things, and processes, that are vulnerable to threats and that we wish to secure. Targets can be classified into several categories:

Types of Targets

1. Resources
 - Air
 - Food Chain (includes plants and animals)
 - Water
 - Energy
2. Infrastructures
 - Built environment
 - Water (supply and control)
 - Energy (e.g., power, gas)
 - Finance system
3. Information, Computers and Communication
 - Computer systems
 - Information sharing systems
 - Public communications (broadcasting)
 - Emergency communications
 - Postal services
 - Networks
4. Transportation



- Air, land, sea
 - Supply Chain
5. Public Health/Safety
 - Public health care system
 - Emergency Services (e.g., fire, ambulance, police)
 6. Industrial Base
 - Refineries, power plants, gas tanks, chemical plants, etc.
 - Any structure that produces potentially hazardous material
 - Nuclear processing facilities
 - Defense supply chain
 7. Government (all levels)
 - Command and control functions
 - Continuity of operations
 - Intelligence/information services
 8. People

Threats are the means by which targets may be subjected to attack and harmed. Threats can be classified into a number of categories:

Types of Threats

1. Explosives
2. Chemical
3. Biological
4. Radiological/nuclear
5. Cyber (Computer viruses, denial of service, hacking, spoofing, identity theft, etc.)
6. Conventional weapons (e.g., handguns, knife)
7. Ordinary physical objects used for attacks (e.g., plane, truck)
8. Human beings (Terrorist groups, criminals)
9. Natural disasters (Earthquakes, fires, floods, storms, etc.)

Countermeasures are the systems, methods and tools used to prevent or respond to threats against targets. Countermeasures can be classified into various categories:

Types of Countermeasures

1. Assessment
2. Protection
3. Detection
4. Identification
5. Response
6. Mitigation
7. Restoration

8. Management

In surveying stakeholder needs and inventorying existing standards programs, the AGS asked respondents to map their inputs to the model described above in order to facilitate identification of areas of coverage and gaps.

5 Stakeholder needs

The AGS determined that a vital component of its review process involved outreaching to security stakeholders to determine their usage of security standards, concerns that they face in the area of security, and whether there are any identifiable gaps where international security standards are needed.

Each of the AGS members performed the stakeholder outreach within their respective country. Members agreed to the following stakeholder questions, to be used for written inquiries or during interviews:

General Standards Questions

1. What standards are the most important to your industry/organization?
2. Do you follow voluntary, consensus standards? Do you follow (or issue) government regulations that reference standards?
3. Do you or any of your associates participate in standards development activities? If so, which ones?

Security Specific Questions

4. What type of security concerns does your organization face?
5. What security standards/guidelines/best practices do you currently use? Are they organization specific, or are they more widely based?
6. If yes, why and how used? Are these national, regional, or international? If no, why not?

Gaps

7. What types of security standards are needed that currently do not exist?
8. Would you consider these needed standards as having an international scope?
9. Have you done a security risk analysis within your industry/association?

The following is a compilation of International Standards Security needs that were identified by respondents to the survey :

Infrastructures (e.g., built environment, finance systems)

- Effective methods to evaluate critical infrastructure vulnerabilities are necessary.
- Office building / Skyscraper safety
- A comprehensive risk management standard that describes the risk management processes and gives guidance about how an organization (especially small to medium sized companies) can achieve that.
- Management system Standard for safety (like ISO 9000 approach).
- An international version of DSTU X9.59 for securing electronic payments.
- An international version of X9.104 draft to support transport of Secure Payment Objects to the ISO 8583/X9.105 environment
- There currently exists a comprehensive set of security standards in the public domain. With that said, the industry needs to be more aggressive in maintaining those standards, given the dynamic threat environment. On the International side, we believe the industry needs to be more aggressive in creating security standards that synthesize the many country specific security requirements.
- Fire Safety Management
- Fire Risk Assessment
- In order to guard the banking system, it is necessary to standardize individual identification, electric certification and risk assessment against money laundering, forged certificate and computer virus.

Resources (e.g., air, water, energy)

- Standards to help protect our energy resources, water, and built environment infrastructures is a priority (vast area).

Information, Computers and Communications

- Control system cyber security standards for risk assessment, equipment specification, security policies
- Security standards that help prevent SPAM.
- Security standards that help prevent phishing.
- Security standards that help prevent spread of computer viruses.
- Industry accepted standards that apply to Security as a whole – this would include information security, personnel security and physical security.
- Security of documents issued by motoring clubs world wide, i.e. Carnet de Passage and International Driving Permits
- We don't have an extension to RFC 2440 supporting multiple digital signatures over an information object or any rules for the order and precedence in such a situation.
- Standards are needed for word processor formats that provide useful coverage, and have software for them available and widely used on the whole range of widely used operating systems. On the whole matter of executables, there should be a clear distinction, in security standards, between execution that can modify the current memory image (in safe

ways), e.g. for printer formatting and display, and execution that can modify files stored externally or execution that has any other communications with the operating system.

- Interoperable DRM solutions are not yet deployed in the market although MPEG IPMPX exist as an international standard. However what we see nowadays is a number of DRM initiatives flourishing to address the problem once more IPDC/DVB-H, DVB TM-SEC, ISMA, OMA, MPEG-21, DMP etc
- Currently, the gap exists in expressing security for distributed authorization services, applications level security services and digital signatures supporting multi-signature and complex XML documents. Many of the emerging standards in OASIS are addressing these gaps such as SAML, XACML, XACML RBAC, SPML and WS Security. Supporting these is a lack of standards for interoperability of authorizations, authorization frameworks although some work in this area is ongoing in ASTM and ISO. ANSI RBAC is new and an ISO version is expected.
- A central depository is needed for all the standards to reside for quick access. Additionally, we are having difficulty finding good software to perform comprehensive facility security audits; imbedding the standards within the program as reference guides.
- Security of security data, especially in respect of vehicle and alarm access codes. Security of internet held data.
- Guideline concerning the system for handling and security of personal information.
- Securing system of 'data input by right and certified person'
- Development and operation of databases, such as 'black list and/or white list'.
- We consider important the combined usage of all required technologies – not only technologies such as biometrics and automatic identification, but also drug-detecting dogs, entrance and exit control, and material control within security areas.
- To establish a biometrical security system, protection profiles should be developed under governmental control. For example, a biometrical system to manage employees within highly secure areas, such as e-passport, Basic Resident Register, IC-carded driver's license.

NOTE - Protection profiles for biometric security are under consideration by ISO/IEC JTC 1/SC 37.

- A personal identification system is required, which checks the identity of the person with the memorized biometric information in the IC memory to enhance identifying accuracy. However once the reference information such as facial image or fingerprint is copied or abused, alternative information will be hard obtain, therefore, we think a guideline of copy protection technologies and of delete technologies, concerning facial information, etc. will be important and early standardization is necessary for risk management and individual information protection.

NOTE - US NIST draft FIPS 201 covers the points raised in this comment.

- The IT security management system standards used in Japan are BS 7799-2 and the ISMS certification standard which are published by the Japan Information Processing Development Corporation. We would like to see BS 7799-2 established as an ISO/IEC Standard as rapidly as possible and integrated with the certification standard.

NOTE - BS 7799-2 is project ISO/IEC FCD 24723 on the ISO/IEC JTC 1/SC 27 work programme.

- Validation Scheme for Cryptographic Modules (related to FIPS140-2).

NOTE -The points raised in this comment is being addressed by ISO/IEC JTC 1/SC 27 with the transformation of NIST FIPS 140-2 into ISO/IEC 19790.

- Validation Schemes for Cryptographic Protocols (such as TLS/SSL, IPsec and other proprietary protocols)

Transportation

- Secure communication technology standards (protect airwaves)
- Intermodal Cargo Containers (supply chain) – screening technologies / inspection standards.
- Reliable Airport Security Standards are of vital importance.
- Port / Marine security assessment & plans (in support of IMO ISPS Code)
- Biometric Technologies is very important in authenticating the identity of travellers.

NOTE - ISO/IEC JTC 1/SC 17 and ICAO are addressing this aspect with the development of a joint project.

Public Health/Safety

- The specific standards that do not exist today include standards for identity management, access or rights management, policy and trust issues, privacy and others.
- There is probably a need for either transport specific or upper layers security profile standards that could be used for those acute care medical devices that use either RF wireless or LAN based transports. This would help ensure interoperability between these devices and existing hospital IT infrastructure without the need for customizing the devices per installation or obtaining additional equipment to provide the needed services.
- Implementable Web services security standards.
- Wireless LAN (in progress)
- Standard for Health Care facilities (protection against infectious diseases)
- Conformance testing

Industrial Base

- Standards concerning trade of chemical materials.
- Management of chemical materials (standard samples, reagents, samples and experimental equipments) is provided by ISO 17025 and so on. We think these standards should be reviewed from a viewpoint of security. The analytical and/or evaluating methodologies concerning biochemical application such as pathogenic germs, detecting pollution existence and cause at emergency situations, standardization of simplified analytical methods and their manipulating manuals are important issues. Moreover rapid analytical methods and detectors of hazardous gases should be standardized.
- Concerning ISO/TC 145 Graphical symbols, we would like to propose that security standards be created covering information on the hazardous materials provided in critical situations, in addition to the information provided by safety color, safety signs and general guides. For example, when a vehicle conveying hazardous materials is involved in a traffic accident, it may create a dangerous situation for first responders. An international guideline on indications, including graphic symbols, is necessary to enable communication at a glance of the relevant information on onboard materials, such as the degree of risk, handling instructions, human body influences, and emergency aid.

Government

- Standards to support public procurement in security field (prevention of corruption)
- The relationship between the military and civilian security and how they can work together and support each other.

People

- Important to be able to deal with the aftermath of an emergency / CBRNE event and provide effective counsel to those affected.
- Standard on how to deal with psychological trauma
- Protecting the first responder community against CBRNE events is a priority. A common set of agreed upon standards are needed in the following areas: PPE – ensemble and equipment (test protocols and performance requirements); Protection against CBRN events, Selection / use / care criteria; Detection equipment requirements; Decontamination standards; Communication Systems (Interoperable)
- Need for agreed-upon set of competencies for first responders / emergency managers (training / education requirements)
- Certification of security equipment (e.g. Detection equipment, PPE, etc)
- Exposure criteria regarding biological materials ; test standards for protective equipment regarding biological agents. Exposure criteria for civil population regarding biological & chemical agents.
- Standards related to CBRN issues. All CBRN related products for personal safety as where dual use is demanded by the consumers.
- Ballistic protective equipment

Managing risks

- An internationally recognized information security management system standards like BS7799.2 is the biggest gap. There are also gaps in areas of measuring and reporting information security status, and guidelines for implementing information security management systems.
NOTE - This point is covered by ISO/IEC JTC 1/SC 27 projects ISO/IEC 24742 and ISO/IEC 24743.
- The anti-theft standard that is being developed in ISO/TC 127 needs to be completed.
- International security standards in the areas of (1) vulnerability assessment methods and measures, (2) risk assessment methods and measures, and (3) health consequences assessment
- There is consensus from many stakeholders that a high-level framework standard is needed to establish a common set of criteria and terminology for preparedness, disaster management, emergency management, and business continuity programs. Such a Standard can provide core organizational planning requirements for: Prevention / mitigation; Preparedness; Response; Recovery; Business continuity.
- Many have expressed a need for a Common / Harmonized Incident Command System to / Coordinate of Federal / Provincial / Local response; Standardize procedures and communications for first responders.

- Global benchmarks for the risk assessment methodology so right amount of security for all hazards can be derived with templates for developing mitigation.
- We don't have actual standards for risk management from a holistic standpoint and are too exposed to risk management by matters of opinion that may be uninformed.

NOTE - ISO/IEC JTC 1/SC 27 is developing security risk management guidelines in ISO/IEC 13335-2.

6 Surveys of existing work of ISO, ITU-T and IEC

6.1 Enquiry on the Inventory of Security Standards in the ISO Technical Committees (see Annex D)

A request was made from the AGS to members of identified security related ISO Technical Committees, asking them to identify any projects in their work programme related to security and to map any such projects to the security framework developed by the AG, see the figure and clause D.1 of Annex D.

The final list of Technical Committees replying is given in clause D.2 of Annex D. As well as those Technical Committees not replying.

The complete inventory with Technical Committees' replies is available at ;
< <http://isotc.iso.ch/livelink/livelink.exe?func=ll&objId=3627201&objAction=browse&sort=name> >.

Based on this input, the AG secretariat mapped all the Technical Committees' inputs of identified projects with the framework security categories.

Clause D.3 of Annex D provides a simple total of projects under each framework category.

On analyzing the input from the Technical Committees, certain gaps can be identified where there is a limited number of projects under development. It should, however, be noted that certain Technical Committees have not provided their input. Others stated they had no security related projects (ISO/TC 192 and ISO/TC 212).

A further analysis of this inventory should be carried out by the SCS (subject to its establishment by the TMB).

6.2 ITU-T

ITU-T has published a manual that provides an overview of the numerous recommendations on security developed by ITU-T (see the AGS N. 40, "[ITU-T Security in Telecommunications and Information Technology \(Version 2004\)](#)");

<<http://isotc.iso.ch/livelink/livelink.exe?func=ll&objId=3515997&objAction=browse&sort=name>>).

6.3 IEC

IEC present development in security work is given in the AGS N. 16, "[Inventory of IEC standards related to Security](#)";

<<http://isotc.iso.ch/livelink/livelink.exe?func=ll&objId=3620343&objAction=browse&sort=name>>.

7 General assessment

Standards play a number of important roles in supporting efforts to achieve security. For example, standards can be used to promulgate best practices and methodologies for security management. Standards can be used to specify test methods and parameters to aid in detection of threats. Standards can specify performance requirements to ensure equipment and systems provide the necessary performance and protection in extreme conditions.

The AGS noted that ISO already has an extensive set of published standards and ongoing development programs related to security. Out of ISO's 205 Technical Committees (including JTC1 subcommittees), 35 have deliverables related to security. Some of these are critical and fundamental to current global efforts to provide security and combat terrorism – recently-developed standards for biometrics, detection of the illicit movement of nuclear material, maritime port security, and security of IT systems are noteworthy examples. These work efforts respond directly to some of the critical needs identified by stakeholders.

There are other areas in which ISO has extensive technical work, but none relating to the security aspects. For example, ISO has technical committees dealing with chemicals, petroleum, and aircraft, but no deliverables relating to the security aspects of these topics. In some instances, petroleum security for example, it was learned that differing regional regulations, and the hesitancy to share security information within the industry, would most likely produce an international standard of little value. For other technical areas, there would likely be benefit from further examination of security aspects.

Many stakeholders voiced the need for a common vocabulary and framework for security management to unify disparate sector-specific approaches, and international standards for emergency preparedness that do not exist today.

ISO's current security work reflects a bottom-up approach to addressing security. This may have been appropriate to a "pre-9/11" world in which terrorism and security threats were viewed as isolated phenomena of mostly local, rather than global concern. Post-9/11, we have come to regard security as a global issue, requiring a systemic approach and "built-in" to societies' infrastructure rather than "bolted-on." ISO requires a more strategic, top-down approach to guide its security-related work. The AGS report contains recommendations for ISO to institute such an approach.

The following section provides the AGS specific recommendations.

8 Recommendations

1. Strategic Focus

Presently, ISO's work on security results almost entirely from "bottom-up" efforts by its Security relevant Technical Committees. This needs to be supplemented with a more strategic, top-down perspective. The AG recommends that the TMB establish a Steering Committee on Security (SCS) to provide continuing strategic direction and coordination of the Technical Committees active in the area of security. The SCS would also provide oversight for any new deliverables received.

2. Guidelines for Technical Committees

Security considerations must become an integral element in the products, systems and operations supporting the day-to-day functioning of society. Accordingly, consideration of security concerns must become an integral part of ISO's process for developing standards. The TMB should establish a joint ISO/IEC working group to develop guidelines to provide direction to Technical Committees on when to incorporate security considerations into their work and what must be considered. SCS should provide oversight for the working group established to develop this guide. A proposed outline of the content of a guide is included in this report (see Annex A).

3. Security Management Standards

ISO should undertake the development of a Security Management System framework standard. This guidance document should provide the common vocabulary, concepts, and principles that underlie an effective system for managing security. It should provide a framework under which sector-specific standards, such as ISO/IEC 17799 for Information Technology, and similar deliverables in other sectors, can be integrated in a cohesive approach to managing security. SCS should provide oversight for the development of the Security Management System Framework Standard. The AGS noted that the TMB has established an advisory group to recommend how ISO should organize its management system standards going forward, and that group may recommend an alternative approach (Note: The preparation of the SMSFS would need to follow ISO Guide 72).

4. Threat (Vulnerability) assessment

The AGS having noted that there is no stand alone "umbrella" document on risk management, recommends that the relevant security related Technical Committees refer to ISO/IEC JTC 1 /SC 27 document ISO/IEC 13335-1 and evaluate similar needs in their area. Further that a clause on "Threat (vulnerability) assessment" be included in the security management system framework standard.

5. Repository of Security Standards (Web Portal)

Many stakeholders indicated that they lack knowledge of what security standards exist and how to obtain them. ISO should establish and maintain a web page that provides a portal to ISO security standards and links to those of other organizations, as well as a roadmap and searchable index to ISO's security deliverables. SCS should provide oversight for the portal.

6. Role of ISO/TC 223

The AGS is concerned about the inactivity of ISO/TC 223 on Civil Defence, whose broad terms of reference include many key aspects of emergency preparedness and response, as well as natural disasters and the urgent need for standards in those areas. The AGS notes positively the Secretariat (GOST-R)'s intention to call a first meeting in 2005 and invite contributions on work program, structure, etc. The AGS recommends that the TMB closely track the progress of TC 223 to ensure a successful start-up. It is also recommended that ISO/TC 223 establish liaisons with the appropriate International Organizations within the scope of ISO/TC 223.

7. Emergency Preparedness Standard

Many stakeholders see an urgent need for a standard on emergency preparedness. It is recommended that ISO develop an International Workshop Agreement (IWA) on this subject in early 2005, building upon existing national or regional standards such as ANSI/NFPA 1600 and deliverables from the Business Continuity Institute UK, e.g. the UK Civil Contingencies Secretariat Disaster Guides. Once developed, this deliverable should be fed into ISO/TC 223 for further progression as a globally relevant International Standard.

8. Built Infrastructure Protection

The AGS notes that ISO TAG 8 coordinates work across ISO/TCs 59, 92, 162 and 145 which provide standards related to buildings. It therefore recommends that TAG 8 be engaged to ensure the correct assignment of work on new technologies to the appropriate Technical Committees. Also as many of the standards date to the 1980's, the AGS recommends that standards for design of buildings be reviewed and updated to make use of the studies done by NIST on the World Trade Center disaster, the applicability of new technologies for rescue from high buildings, natural disasters, etc.

Liaisons should also be established between ISO/TAG 8 (or the relevant ISO/TCs under the TAG) and those International Organizations operating in the area of "Disaster".

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 practises 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

9 Concluding Observation

Security is a matter of urgent global concern. ISO must approach security standards with a high sense of urgency and speed-to-market. The TMB should set an aggressive schedule for the specific deliverables recommended by the AGS to demonstrate that ISO's approach to security is not "business as usual."

The SCS should be established immediately so that ISO does not lose any momentum in ramping up its security work. The security guidelines for TCs should be drafted by end of 1Q2005 and the security standards web portal should be launched during 1Q2005. An International Workshop Agreement deliverable on Emergency Preparedness should be prepared by end of 1H2005 (any standing committee established by the ISO/TMB e.g. SCS should have the responsibility to immediately address the development of a workshop deliverable/standard on International Emergency Preparedness). A Security Management System Framework standard should be drafted by end of 2005.

Finally, the AGS recommends that as ISO TCs consider the recommendations in this report to augment their security-related portfolios, that they make full use of innovative approaches such as IWAs and Partner SDO Agreements, where appropriate, to accelerate availability of their security deliverables.

Annex A

Proposed structure of Guidelines

The following is a proposed draft outline of Guidelines for ISO Technical Committees.

Security Aspects — Guidelines for their inclusion in Standards

Preface/Forward/Introduction

To include background, history, acknowledgements, organizational procedures and requirements, etc.

Example:

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

Guides are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3. Draft Guides adopted by the responsible Committee or Group are circulated to national bodies for voting. Publication as a Guide requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this Guide may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Executive Summary

Discussion of goals

Example:

This guideline was prepared to assist in the development of those standards and protocols which address basic functionality, appropriateness and adequacy for the task, interoperability, efficiency and sustainability. Standards which use this guideline will cover all aspects of security equipment, information analysis, personnel, and systems.

Description of each section

Scope

Example:

This Guide provides standards writers with guidelines for the inclusion of security aspects in standards. It is applicable to any security aspect related to people, property or the environment, or a combination of one or more of these (e.g. people only; people and property; people, property and the environment).

References

Terms and definitions

For the purposes of this Guide, the following terms and definitions apply.

NOTE In other publications slightly different definitions may apply for the same terms, but the concepts are broadly the same.

To include:

- Frequently-used Security Acronyms
- Frequently-used Security Definitions
- Other Terms and Definitions Resources

The Concept of Security

Example:

Security is dealt with in standards work in many different forms across a wide range of technologies and for most products, processes and services. The increasing complexity of products, processes and services entering the market requires that the consideration of security be given a high priority.

General Considerations

Vulnerabilities, Threats, and Risks

- addresses types of vulnerabilities and threats covered in standards and protocols
- discusses risks

Security Framework Requirements

Example:

Types of security standards

Close coordination within and among committees responsible for preparing standards on different products, processes or services is necessary in order to achieve a coherent approach to the treatment of security. The use of a structured approach is recommended to ensure that each specialized standard is restricted to specific aspects and makes reference to wider-ranging standards for all other relevant aspects. The structure is built on the following types of standards:

. basic security standards, comprising fundamental concepts, principles and requirements with regard to general security applicable to a wide range of products, processes and services;

- . group security standards, comprising security applicable to several or a family of similar products, processes or services dealt with by more than one committee, making reference, as far as possible, to basic security standards;
 - . security product standard, comprising security aspect(s) for a specific, or a family of product(s), process(es) or service(s) within the scope of a single committee, making reference, as far as possible, to basic security standards and group security standards;
 - . product standards containing security aspects but which do not deal exclusively with security aspects; these should make reference to basic security standards and group security standards.
- See IEC Guide 104 for a structured approach in the fields of electrical and electronic engineering.

Analysis of proposed new standards

Every proposal for preparing or revising a standard on aspects of security should identify what is to be included in the standard and for whom it is intended. This is usually achieved by answering the following questions.

a) To whom is the standard addressed?

- . Who is going to use the standard and how?
- . What do the users require from the standard?

NOTE The term “users” of the standard includes those implementing the requirements of the standard, those affected by it

(such as consumers of a product or service) and those affected by the environmental impact.

b) What is the purpose of the standard?

Is it to become

- . a basic security standard,
- . a group security standard,
- . a security product standard, or
- . a product standard containing security aspects?

Consider its purpose, as follows.

- . Which aspects relating to security arise?
- . Will the standard be used for testing?
- . Will the standard serve as a basis for conformity assessment? (Full details are given in ISO/IEC Guide 7.)

c) How should the standard be written?

- . What background or knowledge can one assume users of the standard to have?

Preparatory work

Work on a standard starts with the identification of all the security aspects to be covered. At this stage, it is essential to gather all relevant information. A detailed outline should then be prepared which will serve as a basis for the standard.

Before the work of drafting a standard begins, it is necessary to assemble within the committee expertise that reflects the knowledge required to develop the standard. Such knowledge includes, for example, the following:

- . detailed working knowledge of the product, process or service;
- . feedback based on experience by users of the product, process or service;
- . knowledge of the future development of the product, process or service;
- . legal framework. (More details are given in ISO/IEC Directives, Part 2, 1992, subclause 5.1.3.)

Once the content of the standard has been established, the following security aspects should be considered (not all of these may be relevant to a given standard):

- . intended use and reasonably foreseeable misuse;

- . *ability to perform under expected conditions of use;*
- . *environmental compatibility;*
- . *ergonomic factors;*
- . *regulatory requirements;*
- . *existing standards;*
- . *reliability;*
- . *serviceability (including “service maintenance”, such as ease of access to serviceable items, method of refueling/lubrication);*
- . *durability;*
- . *disposability (including any relevant instructions);*
- . *special needs of users [e.g. children (see ISO/IEC Guide 50), elderly people, the disabled] of the product, process or service;*
- . *failure characteristics;*
- . *markings and information.*

Drafting

General

The rules and recommendations given below apply to the drafting of documents intended to become security standards and, whenever applicable, to the inclusion of security aspects in other standards. They are more specific, being either additional or complementary, than those contained in the ISO/IEC Directives, Part 3.

The standard should contain those requirements important in... These requirements should be verifiable and should be laid down

- . *in precise and clearly understandable language, and*
- . *have to be technically correct.*

Standards should contain clear and complete statements specifying methods for verifying that the requirements have been met. Subjective terms or words should not be used unless they are defined in the standard.

Instructions

Instructions and information provided shall cover safe conditions for operating the product, process or service. In the case of products, the instructions shall cover the use, cleaning, maintenance, dismantling and destruction/disposal, as appropriate.

Warning notices

Warning notices shall

- . *be conspicuous, legible, durable and understandable,*
- . *be worded in the official language(s) of the country(ies) where the product, process or service is intended to be used unless one of the languages associated with a particular technical field is more appropriate, and*
- . *be concise and unambiguous.*

Packaging

When relevant, standards shall specify requirements for the packaging of the product, to ensure safe handling of the packed product, to maintain the safety of the product and to eliminate or minimize hazards, including contamination or pollution. In this context, see ISO/IEC Guide 41.

Safety during testing

Standards specifying test methods may prescribe procedures and/or the use of substances or equipment which could create a risk, for example to the laboratory staff. Where relevant, the standard shall include warning statements, as follows:

- . a general warning statement appearing at the beginning of the standard;*
- . specific warning statement(s), as appropriate, preceding the relevant text within the standard.*

NOTE This is in accordance with the ISO/IEC Directives, Part 2, 1992, subclause 6.2.3.

EXAMPLES

a) General warning statement:

CAUTION — Some of the tests specified in this standard involve the use of processes which could lead to a hazardous situation.

b) Specific warning statement:

DANGER — Attention is drawn to the hazard deriving from the use of the sodium salt of fluoroacetic acid, which is an extremely strong poison.

Applications

- end user applications
- management applications

Conclusions**Catalogue of ISO Security-related Recommendations****List of Technical Committees working on Security-related Standards****Bibliography**

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.

Annex C

Summary of Cyber Security Initiatives and Potential Areas for Further International Standards

[ISO/IEC JTC 1/SC 27 – IT Security Techniques](#), is the subcommittee that has already published many international standards on CYBER SECURITY, and continues to develop new projects to meet emerging needs. Its [programme of work](#) lists these standards and projects. Its area of work is 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).

Excluded is the embedding of mechanisms in applications.

It is further noted that the ISO/IEC JTC 1/SC 27 Scope and Area of Work includes the standardization of cryptographic algorithms for integrity, authentication and non-repudiation services. Furthermore it includes the standardization of cryptographic algorithms for confidentiality services for use in accordance with internationally accepted policies.

The US TAG for JTC 1/SC 27 is [INCITS T4](#). They also have a number of [projects](#) in this area.

[ITU-T SG 17](#) and ISO/IEC JTC 1/SC 27 have excellent collaboration on international security standards. For example, three common text standards on security were approved in 2000

- ITU-T X.841 | ISO/IEC 15816
- ITU-T X.842 | ISO/IEC TR 14516
- ITU-T X.843 | ISO/IEC 15945

There is also collaborative work currently underway on a number of new standards:

- ISO/IEC 18028-1 - Information technology -- Security techniques -- IT network security: Network security management
- ISO/IEC 18028-2 - Information technology -- Security techniques -- IT network security: Network security architecture (currently technically aligned with ITU-T X.805)
- ISO/IEC 18028-3 - Information technology -- Security techniques -- IT network security: Securing communications between networks using security gateways
- ISO/IEC 18028-4 - Information technology -- Security techniques -- IT network security: Remote access

- ISO/IEC 18028-5 - Information technology -- Security techniques -- IT network security: Securing communications across networks using Virtual Private Networks

In addition, collaborative work is underway on the revision to ISO/IEC 17799 - Information technology -- Code of practice for information security management. The existing security work in the ITU-T is described in the "[ITU-T Security Manual](#)." The current security work in ITU-T SG 17 going forward is described in [Questions](#) - see Questions E/17 and G/17 through L/17.

Some areas that ISO/IEC JTC 1/SC 27 may want to consider for international standards development, or use as resources for current work, include the following (hyperlinks to actual text of documents or articles on subject):

- [Phishing](#)
- [Cyber Security for Manufacturing Plants](#)
- [Electronic Health Care Infrastructure](#)
- Looking at the work of the [Network Reliability & Interoperability Council \(NRIC\)](#), including prevention [best practices](#) such as:
 - 6-6-8000 "Disable Unnecessary Services"
 - 6-6-8008 "Network Architecture Isolation/Partitioning"
 - 6-6-8015 "Segmenting Management Domains"
 - 6-6-8020 "Security HyperPatching"
 - 6-6-8032 "Patching Practices"
 - 6-6-8034 "Software Patching Policy"
 - 6-6-8037 "System Inventory Maintenance"
 - 6-6-8039 "Patch/Fix Verification"
 - 6-6-8041 "Prevent Network Element Resource Saturation"
 - 6-6-8071 "Threat Awareness"
 - 6-6-8074 "Denial of Service Attack – Target"
 - 6-6-8091 "Validate source addresses"
- [Cyber Security Certification](#)
- US legislation/reports on various cyber issues:
 - The Financial Modernization Act of 1999, also known as the "[Gramm-Leach-Bliley Act](#)" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions.
 - [Healthcare Information Portability and Accountability Act \(HIPAA\)](#)
 - [The US National Strategy to Secure Cyberspace](#)
 - [General Accounting Office \(GAO\)](#) reports on Cyber Security for Critical Infrastructure Protection, Technologies to Secure Federal Systems, and Continued Action Needed to Improve Software Patch Management
- North American Electric Reliability Council (NERC) [Cyber Security Standard](#)
- [Improving Cyber Security of SCADA Networks](#)
- [Common Vulnerabilities In Critical Infrastructure Control Systems](#)
- Virus protection standards
- Spam software standards
- [ISA-SP99, Manufacturing and Control Systems Security Standards](#)

Annex D

Survey of existing work in ISO Technical Committees

D.1 Request to the Security related ISO Technical Committees to complete the ISO/CS enquiry on Security Standards inventory with any "Security projects" on their work programme

ISO Central Secretariat

1, rue de Varembe
Case postale 56
CH -1211 Genève 20
Switzerland

Telephone + 41 22 749 01 11
Fax + 41 22 733 34 30
E-mail central@iso.ch
Web www.iso.ch

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 CONCERNED

Your ref.
Our ref. TMB AGS

Date 2004-06-21

Dear Sir or Madam,

Council, at its meeting in Buenos Aires, recognized that, as a result of events in recent years, the subject of security is high on the list of government priorities as well as being of concern to the general public. It accordingly asked the Secretary-General to engage contacts with relevant international organizations and ISO members and to make an inventory/analysis of all existing security-related ISO standards, with a view to assessing further the needs for International Standards for security and the potential for additional ISO involvement. It was also requested that the Secretary-General refers to the TMB the results of the above action, for consideration of their impact on ISO's technical work. As a result of this, the ISO Technical Management Board, at its January 2004 meeting, approved the establishment of a high-level strategic Advisory Group on Security.

Under the terms of reference, approved by the ISO/TMB, the Advisory Group will:

- Conduct a review of existing ISO deliverables related to the field of security, which may include (but is not limited to) the subjects of:
 - o Training programs and equipment for responders.
 - o Private sector emergency preparedness and business continuity.
 - o Identification techniques, including biometrics.
 - o Emergency communications.
 - o Inter-modal supply chain security.
 - o Risk assessment.
 - o Biological and chemical threat agents.
 - o Cyber security.
 - o Civil defense.



- 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.
- Submit a final report to the ISO/TMB and ISO Council by 31 December 2004.

At its first teleconference the AG on Security developed an inventory of ISO activities relevant to Security and the related Technical Committees.

During the first face to face meeting in June the AG on Security reviewed this list of ISO Technical Committees and mapped it to a framework (categorization) developed by the Advisory Group (see *attachment 1*) to identify areas of coverage.

The resulting categorization of Technical Committees to areas is shown in *attachment 2*.

In order that we may know which standards of your Technical Committee (Subcommittee) are relevant to the areas indicated, we established an inventory of all projects of your work programme and are requesting you to indicate in the column "**Category**" of the inventory the reference areas that relate to each of your ISO projects i.e.

ISO/IEC Reference	ISO Stage	Title	Category
ISO/IEC 7501-1:1997	90.92	Identification cards -- Machine readable travel documents -- Part 1: Machine readable passport	1.3.b, 1.7.c, 2.e

The inventory of your projects is accessible [through this direct link](http://www.iso.org/tmb-ags-enquiry) (<http://www.iso.org/tmb-ags-enquiry>). Please log in with your **current ISOTC username and password**.

Alternatively, you can also access the ISOTC site in the following way :

1. Access ISOTC Portal (www.iso.org/tc)
2. Select "Access to other protected areas" which will display the login screen
3. Select the folder "ISO/CS enquiry on security standards" and **subfolder 1**. "ISO/CS enquiry - List of standards inventory per committee". This folder is located in the upper part of the screen.

As TC secretary we are requesting you to

- **download the file** for your TC from **subfolder 1**. "ISO/CS enquiry - List of standards inventory per committee"
- **complete the column "Category"**
- **upload the modified file** onto the **subfolder 2**. "Committee response to ISO/CS enquiry on standards inventory" **by 23 July 2004**.

We understand that this is a very tight schedule but the TMB AG on Security will need to review the input you provide before their next meeting in September.

Thanking you in advance for your cooperation.

Yours sincerely,



Keith Brannon
TMB AG on Security Secretariat

enclosures

D.2 Status on the ISO/CS enquiry on Security Standards (by 2004-09-13)

ALREADY REPLIED ISO/TCs and ISO/IEC JTC 1/SCs :

JTC 1/SC 17
JTC 1/SC 27
JTC 1/SC 31
JTC 1/SC 37
TC 20
TC 21
TC 34
TC 58
TC 67
TC 68
TC 76
TC 85
TC 92
TC 94
TC 98
TC 104
TC 145
TC 147
TC 146
TC 159
TC 162
TC 192
TC 204
TC 211
TC 212
TC 215
TC 220
TC 224

Note : TC 192 and TC 212 have replied requesting to be excluded from the list.

NOT YET REPLIED ISO/TCs and ISO/IEC JTC 1/SCs :

TC 8
TC 22
TC 28
TC 122
TC 154

TC 190
TC 197

D.3 Standards by Category

Category	Description	Count of Standards
1.	Targets (people, things, processes)	2
1.1.	Resources	1
1.1.a.	Air (TC 146)	117
1.1.b.	Food Chain (includes plants and animals) (TC 34, TC 190)	94
1.1.c.	Water (TC 147, TC 224)	8
1.1.d.	Energy (TC 85)	3
1.2.	Infrastructures	49
1.2.a.	Built environment (TC 92, TC 98, TC 145, TC 162)	162
1.2.b.	Water (supply and control) (TC 224)	3
1.2.c.	Energy (e.g., power, gas) (TC 85, TC 197)	1
1.2.d.	Finance system (TC 68, TC 154)	80
1.3.	Information, Computers and Communication	1
1.3.a.	Computer systems (JTC 1/SC 27)	152
1.3.b.	Information sharing systems (JTC 1/SC 17, JTC 1/SC 27, JTC 1/SC 31, JTC 1/SC 37, TC 204, TC 211, TC 215)	225
1.3.c.	Public communications (broadcasting)	67
1.3.d.	Emergency communications (JTC 1/SC 27, TC 211, TC 215)	93
1.3.e.	Postal services	43
1.3.f.	Networks (JTC 1/SC 27, TC 215)	98
1.4.	Transportation	1
1.4.a.	Air, land, sea (JTC 1/SC 31, TC 8, TC 20, TC 22, TC 58, TC 104, TC 122, TC 154, TC 204, TC 220, TC 211)	838
1.4.b.	Supply Chain (JTC 1/SC 31, TC 8, TC 20, TC 22, TC 58, TC 104, TC 122, TC 154, TC 204, TC 220)	58
1.5.	Public Health/Safety	2
1.5.a.	Public health care system (TC 212, TC 215)	91
1.5.b.	Emergency Services (e.g., fire, ambulance, police) (TC 21, TC 76, TC 94, TC 145)	163
1.6.	Industrial Base	2

Category	Description	Count of Standards
1.6.a.	Refineries, power plants, gas tanks, chemical plants, etc. (TC 28, TC 67, TC 94)	78
1.6.b.	Any structure that produces potentially hazardous material (TC 67, TC 94)	58
1.6.c.	Nuclear processing facilities (TC 85, TC 94)	45
1.6.d.	Defense supply chain (JTC 1/SC 31, TC 94)	35
1.7.	Government (all levels)	1
1.7.a.	Command and control functions (TC 159, TC 211)	30
1.7.b.	Continuity of operations	55
1.7.c.	Intelligence/information services (JTC 1/SC 17, JTC 1/SC 27, TC 204)	55
1.8.	People	59
2.	Threats	1
2.a.	Explosives (TC 98, TC 197)	37
2.b.	Chemical	206
2.c.	Biological (TC 34)	253
2.d.	Radiological/nuclear (TC 85)	29
2.e.	Cyber (JTC 1/SC 17, JTC 1/SC 27, JTC 1/SC 31, JTC 1/SC 37, TC 68, TC 154)	171
2.f.	Physical	58
2.g.	'Ordinary' weapons (e.g., handguns, knife)	19
2.h.	Using physical objects for attacks (e.g., plane, truck) (TC 20, TC 22)	15
2.i.	Human beings	46
2.j.	Terrorist groups (preemptive protection) (TC 68), identify theft (JTC 1/SC 17, JTC 1/SC 37)	64
2.k.	Natural disasters (TC 8, TC 21, TC 98, TC 211)	34
2.l.	Earthquakes, fires, floods, storms	202
2.m.	Computer viruses, denial of service, hacking, spoofing	1
3.	Key Aspects: Managing Risks	1
3.a.	Threat/Vulnerability assessment (TC 68, TC 211)	205
3.b.	Protection (JTC 1/SC 27, TC 21, TC 85, TC 92, TC 94, TC 98, TC 145, TC 159, TC 162, TC 197)	422
3.c.	Detection (TC 22, TC 34, TC 85, TC 104, TC 154, TC 146, TC 147, TC 192, TC 211, TC 224)	323
3.d.	Response (TC 8, TC 21, TC 94, TC 159, TC 215)	93
3.e.	Mitigation (prevention and containment) (TC 8, TC 22, TC 98, TC 146, TC 147, TC 192, TC 224)	106
3.f.	Restoration/recovery	50



Category	Description	Count of Standards
3.g.	Management systems (culture and processes) (JTC 1/SC 27)	72
3.h.	Forensics/attribution	7
3.i.	Identification/authentication (JTC 1/SC 17, JTC 1/SC 31, JTC 1/SC 37, TC 20, TC 68, TC 104, TC 204, TC 215)	398