ISO/IEC JTC 1 N9828

2009-09-30

Replaces:

ISO/IEC JTC 1
Information Technology

Document Type:	other (defined)
Document Title:	JTC 1 Correspondance to the ISO/TMB AGS
Document Source:	JTC 1 Chairman
Project Number:	
Document Status:	This document is forwarded to JTC 1 National Bodies for information.
Action ID:	FYI
Due Date:	
No. of Pages:	6

ISO/IEC JTC 1 is pleased to respond to the request by the ISO/TMB AGS to provide feedback on the recommendations 9 to 15 as outlined in the letter of the 16th October 2008 from the Secretary of the AGS. JTC 1 responses were requested for the Advisory Group's recommendations as captured in Resolution 11 (Personal Identification), Resolution 12 (Cybersecurity) and Resolution 15 (Transportation systems). Please note that ISO/IEC JTC 1/SC 27 is also involved in work that could be useful to Recommendations 13 and 14. (These comments are contained in the latter part of the Resolution 15 response.)

General ISO/IEC JTC 1/SC 27 Response

ISO/IEC JTC 1/SC 27 has recognized many areas of critical importance regarding the protection of information including:

- Information security risk management, incident management, metrics and measurements;
- Information security governance;
- Information security assurance;
- Cyber-security;
- Identity management and privacy;
- Protecting the electronic frontiers, processes and applications businesses and government are so dependent on both globally and nationally;
- Protecting national infrastructures and their critical elements e.g. telecoms, healthcare, transportation, food supply, finance, utilities, emergency services and government services.

In response to this recognition and commensurate with this knowledge and understanding based on feedback from NBs, liaison organizations and user feedback from around the world, ISO/IEC JTC 1/SC 27 continues to shape its standards development programme to meet the immediate demands of business, business sectors and government. This response is clearly evident from inspection of the current SC 27 work programme given in Standing Document (SD) 4 and its awareness document SD11.

By establishing greater awareness and cooperation between all TCs and the work of JTC 1 SCs, the ISO community could benefit and share from many of these important developments, as well as reduce or eliminate possible duplications and contradictions.

In addition to SC 27 expanding its programme of work, it has also recently adopted the following **revised scope**:

The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- *Security requirements capture methodology;*
- *Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;*
- *Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;*
- *Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;*
- *Security aspects of identity management, biometrics and privacy;*
- *Conformance assessment, accreditation and auditing requirements in the area of information security;*

• Security evaluation criteria and methodology.
SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.

11. Personal identification

ISO/IEC JTC 1/SC 27 Response
SC 27 has recognized that the area of identity management and privacy protection are two pressing areas of concern in particular regarding the wide-spread growth in risks related to the use of Web technologies by both business users and citizens. To deal with this issue SC 27 established, a few years ago, a new working group to deal with this issue (SC 27/WG 5).

With regard to work on identity management SC 27 has a number of relevant projects underway, including:

- ISO/IEC 24745 Biometric template protection
- ISO/IEC 24760 A framework for identity management
- ISO/IEC 24761 Authentication context for biometrics
- ISO/IEC 29100 Privacy framework
- ISO/IEC 29101 Privacy reference architecture
- ISO/IEC 29115 Entity authentication assurance
- ISO/IEC 29146 A framework for access management

These projects are at various levels of development and maturity but expectations are that they will deliver standards over the next 1-3 years.

Additional work being planned within SC 27 includes:

- NWIP on “Privacy Capability Maturity Model”
- NWIP on “Requirements on relative anonymity with identity escrow - model for authentication and authorization using group signatures”

There is also SC 27 work in the development of security methods, techniques and mechanisms to support the implementation of the standards listed above such as encryption, digital signature and authentication standards.

The collective scope of this work should cover the requirements of Recommendation 11.

ISO/IEC JTC 1/SC 37 Response
JTC 1/SC 37 agrees with ISO/IEC/ITU Strategic AGS that Personal Identification is an extremely important area of standardization. Since its inception in July 2002 JTC 1/SC 37 has maintained an accelerated pace of development. JTC 1/SC 37 has completed the first generation of biometric standards (e.g., biometric data interchange formats, technical interfaces and performance testing and reporting standards) and is developing the second generation of these standards as well as other related standards (e.g., biometric sample quality) with the goal of improving the existing standards, adding functionality and reflecting technology innovations and new customers’ needs for biometric-based personal identification applications.

In addition, JTC 1/SC 37 is developing a harmonized biometric vocabulary, biometric data interchange formats for other modalities (i.e., voice data and DNA data), a multi-part project to specify conformance testing methodology standards for the biometric data interchange formats and cross-jurisdictional and societal issues-related projects (e.g., use of biometric technology in commercial ID Management applications and processes, pictograms, icons and symbols for use with biometric systems).

Since SC 37's inception, twenty-four standards and three Technical Reports have been published. Accounting for amendment projects, the revision of existing standards and new projects, the SC 37 PoW currently includes twenty projects subdivided into sixty-seven subprojects.

JTC 1/SC 37 works very closely with JTC 1/SC 17 and SC 27 through active liaison relationships dedicated experts teams focused on the harmonization of biometric, token and security standards. These activities demonstrate the excellent communication and cooperation between JTC 1/SC 37 and these two other JTC 1/SCs. The technologies addressed by JTC 1/SC 17 and SC 37 are, for some applications, complementary in nature. The potential contributions that SC 37 can make to SC 17 through this liaison activity are substantial, particularly in the specification on the use of biometric data within their projects. The complementary nature of JTC 1/SC 27 and SC 37 projects facilitates close and anticipated long-term collaboration between experts from both SCs and a strong spirit of cooperation exist.

12. Cybersecurity

ISO/IEC JTC 1/SC 27 Response

With regard to work on cyber security issues and with specific interest in the potential "gap" areas identified in Annex C of the security report AGS N46, SC 27 has for a long time been particularly mindful of the seriousness of the risks of cyber attacks to both business users and citizens. In recognition of this serious problem, SC 27 has a number of relevant cyber security projects including:

• ISO/IEC 27031, Guidelines on ICT readiness for business continuity.
• ISO/IEC 27032, Guideline for cyber-security
• ISO/IEC 27033, Network security (revision of ISO/IEC 18028:2006)
o *Part 1: Guidelines for network security*
o *Part 2: Guidelines for the design and implementation of network security*
o *Part 3: Reference network scenarios -- Risks, design techniques and control issues*
o *Part 4: Securing communications between networks using security gateways – Risks, design techniques and control issues*
o *Part 5: Securing virtual private networks – Risks, design techniques and control issues*
o *Part 6: IP convergence*
o *Part 7: Wireless*
• ISO/IEC 27034, Applications security
• ISO/IEC 27035, Information security incident management, (revision of TR 18044 + Annex Categorization & Classification of incidents
• ISO/IEC 29147, Responsible vulnerability disclosure

These projects are at various levels of development and maturity but expectations are that they will deliver standards over the next 1-3 years.

Additional work being planned within SC 27 includes:

• NWIP on "Guidelines for identification, collection and/or acquisition and preservation of digital evidence
• NWIP on "Guidelines for security of outsourcing"

There is also SC 27 work in the development of information security assurance and system security evaluation standards. The collective scope of this work should cover most of the immediate requirements of Recommendation 12. However, there are some requirements that NBs feel are not appropriate to SC 27, in particular to develop standards concerning 'cyber security certification' because the timeframes for responses to changed cyber threats is inconsistent with the timeframes for the development of ISO/IEC standards.

15. Transportation systems

General JTC 1 Response

JTC 1 SCs 17 and 27 would welcome the opportunity to coordinate with TC 204 and, per the Advisory Group's recommendation 53, the JTC 1 SCs would be happy to expedite any requests for liaison from TC 204.

ISO/IEC JTC 1/SC 17 Response

SC 17 operates within the time frames contained in the directives and actively seeks to utilise the fastest method to market wherever possible within the confines of producing reliable, well formed standards. The process is, of course, governed by the need to maintain consensus. Our primary standard in this area, Machine Readable Travel Documents (MRTD) is ICAO 9303, being fast tracked through WG4. SC 17 experts provide significant expertise to the formulating group within ICAO. SC 17 will shortly be starting the short form endorsement of part 3 of ICAO 9303 which covers ID1 size MRTD's, which is being utilised as the ID cards standard, for example in the UK.

ISO/IEC JTC 1/SC 27 Response

Protecting the critical infrastructure as well as security standards for sector specific requirements are two recent fields of involvement for SC 27. These areas of work are of growing concern to NBs and organizations around the world, as inter-dependencies between infrastructure elements increase and there are a greater number of points of failure being discovered.

As this area of work is complex, it requires a greater level of cooperation, coordination and expertise from many other fields of expertise. Critical Infrastructure is a challenge to all TCs and JTC 1 SCs, hence SC27 feels that there should be a greater involvement from TMB AGS in these respects.

In response to recommendations 13-15 inclusive, the following is an indication of SC 27 progress and developments that address generic sector requirements as well as sector specific requirements including critical infrastructure elements:

Published standards

- ISO/IEC 27001, Information security management system requirements
- ISO/IEC 27002, Code of practice for information security management
- ISO/IEC 27005, Information security management system risk management
- ISO/IEC 27011, Telecoms requirements for information security management

Standards under development

- ISO/IEC 27003, Information security management system implementation guidance;
- ISO/IEC 27004, Information security management measurements;

- ISO/IEC 27010, Information security management for inter-sector communications (this includes work on SCADA);
- ISO/IEC 27012, Information security management systems for e-government.

NWIP

- Information security management systems for Financial and Insurance Services Sector;
- Guidelines for the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001 (i.e. integrated service management with information security management);
- Information security governance framework.

In all cases of sector specific standards, SC 27’s role is one of support to the relevant TC that is responsible for that sector. For example, the topic of electronic health care is highly specialised and so any SC 27 work on electronic health care infrastructure should be done in close liaison with TC 215. It would be valuable for ISO TC 204 to establish liaison with SC27 to work collaboratively on information security for transportation systems.

A good example of an effective standardization partnership was during the development of the telecommunication information security management standard, ISO/IEC 27011 which was done as a collaborative project with ITU-T.

In this way, concerning the protection requirements for manufacturing and process control, SC 27 has insufficient links with organisations involved in these areas hence such work would be better done in liaison with TCs which focus on the relevant sector requirements to produce credible standards in the area of manufacturing plants, process control and SCADA.

On the question of specific vulnerabilities and government requirements in critical infrastructure control systems, this is a matter that is currently being considered by governments at a national level and so the scope of the work of SC 27 in these areas is accordingly limited.