ANSI-NASPO

Guide 72 Study Report
for a
Security Assurance MSS

November 5, 2009

Table of Contents

1.0 INTRODUCTION

The study reported in this document was carried out by :-

- The American National Standards Institution (ANSI)
- The North American Security Products Organization (NASPO)

in accordance with ISO/IEC Directives Part 1:2001 and ISO Guide 72:2001 (E).
The study reported has examined the need for and impacts of an international security assurance standard.

1.1 What is Security Assurance and how does it compare with Quality Assurance?

Assurance of both quality and security is the act of providing individuals and organizations that rely on them with a measure of confidence, certainty and trust. Assuring quality is doing what it takes to convince relying parties that persons, machines and infrastructure will be able to perform consistently and reliably such that quality does not fall below an agreed threshold. For quality, this means that the effects of mistakes and occasional degradation in performance of

- honest people ,
- who follow the rules,
- who respect the feelings of one another and
- who perform an honest days work for what they earn,

must be taken into account and effectively offset by acceptable measures taken by quality assurance management to avoid falling below the required quality threshold.
Security on the other hand is the opposite. Security is dealing with the effects of willful acts of fraud and crime carried out by

- dishonest and harmful people,
- who break the rules,
- who do not respect the feelings and will knowingly do harm to fellow citizens and
- who do not perform an honest days work for what they earn.

Assuring security is doing what it takes to convince relying parties, often in advance of assuring quality, that the risk of the effects of dishonest and harmful acts does not rise above an agreed threshold.
Assuring security is the process of understanding the nature and likelihood of threats posed by those who commit harmful and dishonest acts and guarding against them by using specially trained personnel, special (security) systems and infrastructure to deter, detect and control their effects to the satisfaction of the relying party. The proposed MSS addresses these threats and sets standards that a relying party can use to specify and communicate the level above which the risks must not rise. The measures taken by security management to ensure that these risks do not rise above a set threshold and the improvements that are introduced to lower them, should follow the classical “Plan, Do, Check, Act” principles of quality assurance. Understanding the threats posed by harmful and dishonest individuals and organizations and setting an acceptable risk threshold to rely on requires subject matter expertise and methods of expression and precaution that are outside the realms of what is normally expected of quality assurance. For these reasons, the study team who have prepared this report believe that security assurance is a separate subject matter area that requires a distinct family of international standards to serve the growing market of supply and demand for security assurance. The proposed MSS will enable those who demand security assurance to better specify their requirements and verify delivery without creating a roadmap helpful to the threat perpetrators. For suppliers, the MSS will clearly communicate the risk threshold and the management needs of the relying parties and the evidence they will need to assure the relying party.
The ultimate objective of the creation of this internationally recognized security assurance standard is to enable the providers of goods and services to satisfy both a quality assurance

level and a security assurance level in the manufacture and supply of their products and services.

Hopefully, the content of this report will convince those reading it to conclude likewise.

1.2 Terms of Reference of the Justification Study

The study reported has examined ISO/IEC Directives Part 1:2001 and ISO Guide 72:2001 and concluded that the principles and criteria for justification expressed in these documents must be satisfied in their entirety. Accordingly, this report has been structured to respond first to a demonstration of compliance with the stated principles followed by a response to the criteria (questions) specified in Annex A of Guide 72. This report is considered to be a part of and is accompanied by a NWIP to ISO/TC 247 on Fraud Countermeasures and Controls for the development of a security assurance MSS.

2.0 Principles for the Justification of an ISO MSS

ISO/IEC Directives Part 1:2001 and section 5 of Guide 72 state that an MSS should be initiated, developed and maintained only when all of the following principles are observed. In the section that follows members of this study team provide their assessment of the degree to which each is observed.

2.1 Market Relevance

The assessment of this study team is that a security assurance MSS has strong and growing market relevance. This assessment is based upon the coming into existence of the:-

- ANSI/NASPO security assurance standard in North America the,
- CEN CWA security management system for security printing in Europe and the
- ISO technical committee on fraud countermeasures and controls – ISO/TC 247,

and a growing demand within governments, societies, industries and service providers for real evidence that the risk of fraudulent acts (caused by dishonest and harmful people) does not rise above an acceptable threshold. This applies to food, water, energy, health care, prescription drugs, travel, transportation, personal identity, personal permission, access permission and all products, services, privileges and entitlements that are subject to serious threats posed by harmful and dishonest individuals and organizations. The setting of those risk thresholds, how they are set, how evidence of managing to keep them from rising above the thresholds are assembled and provided are the subject of the proposed security assurance MSS.

The conclusion of this study team is that markets everywhere are increasingly being subjected to these threats, acts and their effects. A strong security assurance MSS, if implemented widely across affected markets, will contribute significantly to reducing their abuse in the same way that wide adoption of quality assurance has instilled trust in delivery of that property.

2.2 Compatibility

This study team has found no major reason to suspect that a security assurance MSS will be incompatible with any existing ISO quality assurance or ISO/IEC risk management standards. On the contrary, every effort will be made to ensure that this does not happen. To this end, the guidelines for development and presentation of an MSS contained in ISO GUIDE 72:2001 (E) will be followed. Normative reference will be made whenever possible to minimize the need for duplication. The effort, skill sets and liaison with other TC's essential to meeting this objective are made explicit in the NWIP that accompanies this study. In particular, we recognize the need to :-

- emphasize that implementation of security assurance measures must follow the PDCA principles of quality assurance that are manifested in ISO 9001,
- work closely with ISO/IEC JTC-1 and its' subcommittees to ensure that information technology risk management requirements are properly referenced and integrated into the assurance MSS,
- work closely with ISO/TC 8 and its' subcommittees to ensure that supply chain risk management requirements are properly referenced and integrated into the security assurance MSS and
- work closely with the ISO working group that has developed the social responsibility guideline ISO 26000 due to be released in 2010.

The one and only area of potential incompatibility identified by the study team concerns achievement of balance between the need to avoid provision of unintended assistance to perpetrators of fraudulent acts and the ISO requirement, of every MSS, to obey the fundamental principles of clarity and avoidance of ambiguity and obscurity. ISO/TC 247 must ensure that all fraud countermeasure and control standards that it develops achieve this balance. To this end, the NWIP that accompanies this justification study, highlights the need for ISO/TC 247 to review past policies and practices in this sensitive area of standardization and reaffirm or formulate new policy if none are found that satisfy the criteria for this kind of balance.

2.3 Ease of Use

The study team has carefully studied the American national security assurance standard that ANSI and NASPO is proposing be used as the foundation document for this MSS and consulted many of its' users. As a result, the study team has found a consensus of opinion that confirms ease of use of this standard. The assessment of the study team is that the content and structure of the American national standard achieves ease of use. Hence, if the proposed MSS uses the example of the ANSI/NASPO security assurance standard the study team believes that the ease of use objective should be met.

2.4 Topic Coverage

The principles of security assurance that must be covered in the proposed MSS, will be generally applicable to all markets and industries. The study team foresees the need to annex to the generic standard, industry or sector specific requirements that cover the unique requirements of those industries or sectors. The NWIP, that accompanies this study, has identified a number of industries and types of operation that have unique requirements that may be covered in this way. They include, for example, the security printing, customs and border operations and operations that are the custodians of personally verifiable information (PII). Annexed in this way to the generic MSS, the study team believes that the objective to minimize the issuance of separate sector specific versions of the MSS will be met.

2.5 Flexibility

The proposed security assurance MSS will, by design, have built in flexibility. Users will be able to select from a variety of assurance levels to suit their need and implement their own solutions that comply with the performance requirements. The assurance levels are expected to range from basic to very high. Best security assurance practices may be indicated in the standard but how to comply with the requirements will remain open to the organization seeking to assure security. Based upon the choice of assurance level and implementation openness built into the proposed

MSS, the study team believe that the flexibility objective will be met.

2.6 Technically Sound Basis

Modern security assurance relies for its' effectiveness on a combination of technology and human factors with tradeoffs to be made between them by the use of security management principles. Those experienced in security assurance have made these tradeoffs and evolved recognized best management and assurance practices in the face of ever evolving and mutating threats. Technology abounds from biometric access control to GPS used to locate and track transportation. The MSS proposed will be developed by those who are cognizant of this technology but at the same time well aware of the tradeoffs involved in this special area of management. The understanding of the study team, of the purpose of this principle, is that it requires an MSS to be based upon proven management practices and/or scientifically validated and relevant data. The proposed MSS is based upon an American national standard that has undergone five years of use as a national standard and three years as an industry standard. This standard has also been through two national consensus reviews, the most recent within the last year including an update within the last year, Based upon this experience the study team believes that the requirement for a proven management practice will be met. On the conformity assessment side, the study team believes likewise, that the methods of verification of compliance with the American national standard (which has also undergone eight years of use) that are based upon the use of objective evidence, combined with an element of adjudication (as to whether or not security risk management objectives are actually being met), are also consistent with this principle and will be met.

2.7 Easily Understood

Use of plain English should maximize ease of understanding and ease of translation into other languages. Use of diagrams, such as decision and logic trees and tabulations whenever possible should also foster understanding in other languages. It is imperative that the intent of all requirements in the MSS be made clear and unambiguous but, as we have noted above, care must be taken to avoid attracting and assisting the threat perpetrators to plan and optimize their attacks. The study team believes that by establishing avoidance criteria that do not subtract from the communication of the intent, a means can be established to satisfy both ease of understanding and support avoidance of fraud assistance objectives. Again, to the extent that the American national standard has been successfully used by businesses in other cultures and languages, the study team believes that the proposed MSS, will also be understandable.

2.8 Free Trade

Stringent anti trust laws in the United States compel the proposers of this MSS, ANSI and NASPO to guard against the creation of actual or perceived barriers to trade in all American national standards they develop and approve. The American national security assurance standard is open, publicly available and judged by anti trust legal experts to be consistent with US anti trust law. The risk of creating trade barriers, in the opinion of the study team, lies more in the policies, procedures and practices of assessing conformity than in the standard document. For this reason special attention is paid by the American certification body to base assessment of conformity on objective and verified evidence of compliance in order to avoid both actual or perceived bias in the result. One exception to this rule, of openness and avoidance of bias, concerns fraudulent organizations. Those accredited to certify to the American national standard

and hopefully to the proposed MSS, are required to perform due diligence on all certification applicants to verify that they are bona fide and not fraudulent. In other words, assessment of security assurance conformity and certification are not open to fraudulent individuals and organizations. In summary, the study team believes that the proposed MSS will create no technical, procedural or other barriers to trade that would be in violation of any WTO agreements.

2.9 Applicability of Conformity

Nothing is envisaged in this proposed MSS that would preclude either first, second or third party assessment of conformity. Likewise, nothing is envisaged that would preclude joint assessment of conformity with, for example, quality assurance, information technology or supply chain risk management requirements. On the contrary, it is logical for this be encouraged and to the extent that this can be done in the proposed MSS it will be encouraged. Experience with assessment of conformity with the existing American national security assurance standard indicates that the majority of relying parties prefer third party assessment. Some, however do it themselves (second party) and some rely on self assessment (first party).

In summary this study team asserts that joint audits will be encouraged by the proposed MSS to the extent possible and nothing intrinsic to the MSS will preclude the choice of either first, second or third party assessment. The study team, in addition, strongly recommend that the secretariat of ISO/TC 247 begins now to plan for the need that will eventually arise for subject matter competence to be made available to national accreditation bodies in anticipation of their need to accredit third party certification bodies.

2.10 Exclusions

The proposed MSS will use the example of the American national security assurance standard and other MSS documents such as the 27000 and 28000 series to absolutely avoid specification of directly related product or services produced or delivered by organizations who implement this MSS. This study team acknowledges their clear understanding of the need for these exclusions and warrants that this MSS will comply.

3.0 Answers prepared by the Study Team to the Justification Criteria Questions Raised in Annex A of ISO Guide 72:2001 (E)

A.2.1 Basic information on the MSS proposal

a) What is the proposed purpose and scope of the MSS?

PURPOSE

The overarching purpose of the proposed MSS is to enable organizations to maintain value in products, information and services by creating significant barriers to fraudulent acts that have the potential to cause end users and consumers to lose confidence and trust in those products, information and services.

The MSS proposed by this NWIP will enable parties relying on secure operations, to manage all security risk by specifying requirements and best practices to be implemented that will assure an acceptable level of resistance to acts or threats posed by harmful or fraudulent individuals and organizations. The purpose of requiring an acceptable level of resistance to these acts or threats is to maintain integrity of the secure operation in spite of the acts or

threats posed. The operations of security solution and authentication solution providers are examples where security assurance is required to both obtain and maintain efficacy of those solutions.

SCOPE

The MSS proposed by this NWIP is relevant to :

- all parties who rely on security and secure operations,
- countering and controlling all risks caused by, or resulting from, a lack of resistance to the acts or threats posed by harmful or fraudulent individuals and organizations,
- minimizing the effects of all breaches of security if and when they occur.

The intent is that this MSS will offer relying parties the option of specifying security risk management requirements that will assure security at varying levels of assurance ranging from a basic to an extremely high level. As well, the intent is to structure this MSS into a generic version with annexes or serial versions that cover the unique requirements of specific industries and/or extraordinary operations.

The scope explicitly excludes security assurance requirements related to national defense or security related governmental entities.

b) Would the proposed MSS work item result in an International Standard (IS), an ISO(/IEC) Guide, a Technical Specification (TS), a Technical Report (TR), a Publicly Available Specification (PAS), or an International Workshop Agreement (IWA)?

The intent is that this NWIP will result in an International Standard (IS).

c) Does the proposed purpose or scope include product (including service) specifications, product test methods, product performance levels, or other forms of guidance or requirements directly related to products produced or provided by the implementing organization?

No.

d) Is there one or more existing ISO technical committee or non-ISO organization that could logically have responsibility for the proposed MSS? If so, identify.

Yes, the newly formed ISO technical committee TC 247 Fraud Countermeasures and controls.

e) Have relevant reference materials been identified, such as existing guidelines or established practices?

Yes. This NWI proposes that the American national standard, ANSI/NASPO-SA-2008 Security Assurance Standard form the basis of the proposed new MSS. The NWIP anticipates that this existing ANSI/NASPO standard will be modified :

a) to make normative reference to relevant ISO/IEC security standards and
b) to make it valid for all member nations of ISO.

f) Are there technical experts available to support the standardization work? Are the technical experts direct representatives of the affected parties from the different geographical regions?

Yes. Technical experts are available from both the “P” and “O” members of TC 247. In particular, those experts within the USA who were responsible for formulation and implementation of the American national standard are available as well as subject matter experts previously involved in the development of a similar CEN workshop agreement who are now participating in TC 247 and PC 246.

g) What efforts are anticipated as being necessary to develop the document in terms of experts needed and number/duration of meetings?

Experts are needed in the areas of :-

a) The national laws and regulations of ISO member nations that must be taken into account when the effort is made to render the existing ANSI/NASPO standard internationally valid.
b) Establishing the relevance of existing ISO/IEC management standards for consideration as normative references.
c) Fraud countermeasures and controls when the effort is made to :-
    - identity new or unusual forms of threat that must be taken into account
    - carry out a detailed review and approval of the applicability of all existing requirements and best practices specified in the proposed reference document - the ANSI/NASPO security assurance standard.
d) Fraud countermeasures and controls when the effort is made to formulate ISO/TC 247 policy and procedure concerning methods of specification and interpretation that avoid :-
    - unintended invitations of attack and
    - unintended provision of information that will enable the planning and optimization of attacks by harmful or fraudulent individuals and organizations.
e) Fraud countermeasures and controls when the effort is made to address and annex unique MSS needs in the areas of specific industries and extraordinary operations which may not be addressed by the generic MSS.

Over the course of the 3 year period planned for completion of this MSS, it is estimated that :-

a) One 3-day meeting will be required to launch the working group formed to develop this proposed new MSS. This kick-off meeting will be followed in the first year by a second 3-day face to face meeting. In the second and third years of this project it is anticipated that two (2) meetings each of 2-3 days duration will be required to successfully progress the project and provide the level of communication that face to face meetings uniquely provide. The number of members of the working group shall be reasonably limited based upon the work program of the group.
b) Between meetings it is anticipated that regular monthly or bi-weekly conference calls will be made to facilitate essential communication, discussion and resolution of issues.
c) In the first year it is estimated that the project leader can expect to devote, on average, 1-day per week to this project and half a day per week in the second and third years. In the first year, the intensity of effort of the project leader is expected to be significantly higher in the first half of the year.
d) The pattern of effort of some members of the working group is expected to be similar to that of the project leader. The actual level of effort will be dependent upon the nature of the effort and complexity of issues that arise. At most, members of the working group can expect to devote 1-day per week to this project and half a day per week in the second and third years.

h) What is the anticipated completion date?

Dec 31, 2012

A.2.2 Affected parties

a) Have all the affected parties been identified? Yes. For example:

1) organizations (of various types and sizes): the decision-makers within an organization who approve work to implement and achieve conformance to the MSS;

Within organizations of various types and sizes we believe that the decision makers who will approve investments in security infrastructure, systems and work to implement and achieve conformance to this new MSS have been identified. Identification has come from operation, since 2004, of the conformity assessment program by NASPO for certified compliance with the ANSI/NASPO security assurance standard. The decision makers are those within these organizations who see value in compliance and are authorized to act accordingly. The decision makers are security directors/managers, marketing managers, sales managers and in some cases the owners. They are motivated to certify by the need for competitive advantage (or avoidance of competitive disadvantage), compliance with customer security assurance requirements, a desire to show improvements in security and in some cases an internally driven need for an independent assessment of their security assurance attainment. It is expected that the same types of decision makers will be found in organizations in other parts of the world. Certifications carried out by NASPO in Japan, Germany, France and Singapore appear to confirm this expectation.

2) customers/end-users, i.e. individuals or parties that pay for or use a product (including service) from an organization;

   Affected parties identified in this group include government agencies, multinational corporations and security technology integrators who are responsible for procurement of security solutions, authentication solutions or technologies and restricted to contracting only with suppliers/providers who meet specific security assurance requirements. The consensus body that updated the ANSI/NASPO security assurance standard (from the original 2005 version to the present 2008 version) was made up of User, Producer/Provider and General Interest stakeholder groups. Members of the ANSI/NASPO consensus body-user group are all parties that pay for and use a product or service from an organization. It is expected that a similar user group will be formed to ensure balance within the body formed to reach consensus on the MSS proposed by this NWIP.

3) Supplier organizations, e.g. producer, distributor, retailer or vendor of a product, or a provider of a service or information;

   Affected parties identified in this group include all supplier/provider organizations who are required by their customers/buyers to comply with security assurance requirements. Reasons for this requirement are normally based on customers/buyer knowledge that supplier/provider organizations are exposed to the risk of attack and consequently that their personnel, their suppliers and their property need protection.

   Examples of supplier/provider organizations include security solution providers, authentication solution providers, secure document issuing authorities and security technology providers and integrators.

   The consensus body that updated the ANSI/NASPO security assurance standard (from the original 2005 version to the present 2008 version) included a Producer/Provider stakeholder group of affected parties. Members of the ANSI/NASPO consensus body-Producer/Provider group are all parties that supply/provide a security product or service. It is expected that a similar Producer/Provider group will be formed to ensure balance within the body formed to reach consensus on the MSS proposed by this NWIP.

4) MSS service provider, e.g. MSS certification bodies, accreditation bodies or consultants;

   - Certification bodies identified include all major international bodies such as TUV Rheinland Group, SGS and DQS among others.
   - Accreditation bodies identified include all national MSS accreditation bodies such as

ANAB in the USA, BSI in the UK, and SCC in Canada among others.
- Consultants identified include ASIS in the USA, VPGI in the Netherlands and QConsult in the Philippines among others

5) regulatory bodies;

Regulatory bodies interested and affected by this proposed new MSS include government agencies of all ISO member nations who require regulated industries or organizations to comply with security assurance requirements. The regulatory bodies identified include those who regulate :-

- Issuers of identity and travel documents
- Prescription drug manufacturers, their suppliers and supply networks
- Access to secure computer networks
- Access to secure facilities
- Enrollment of individuals and entities into identity management systems
- Critical component supply networks
- etc

6) non-governmental organizations.

No operational or advocacy NGO's (as defined by the World Bank) have been identified as affected at this time. Several citizen advocacy groups, such as the San Francisco based Center for Democracy & Technology and American Civil Liberties Union in the USA and similar NGO's elsewhere in the world are expected to take an interest in this MSS because reduction in the security risk of personnel involves the conduct of background checks that to some, appear to be an invasion of personal privacy. As a result these types of NGO's will be treated as affected parties and serious consideration given to their participation in the international consensus body formed to create this new MSS.

b) Is the MSS intended to be a guidance document, contractual specification or regulatory specification for an organization?

The proposed MSS sets standards for assuring a level of security of operations. The standard upon which this proposal is based is the American national standard, ANSI/NASPO-SA-2008 Security Assurance Standard. This American national standard was introduced in 2005 and has since been adopted by :-

- the US Department of Homeland Security as a guideline to be followed by State authorities who issue driving licenses and ID cards,
- the US Government Printing Office for use in procurement specifications as a mandatory requirement for suppliers of document security components,
- multinational corporations such as Intel, HP, Johnson & Johnson, Bristol Myers Squibb et al, both as a guideline for internal use and security solution suppliers to follow and in some cases as a mandatory contract condition,
- the Semiconductor Industries Association (SIA) and Semiconductor Equipment and Materials International (SEMI) as an essential qualification for Authentication Service Providers (ASP's) who are a critical component of the authentication system defined in the SEMI standard "DETECTING AND PREVENTING COUNTERFEITING OF SEMICONDUCTORS AND RELATED PRODUCTS",
- Security solution providers in the USA, Germany, France, Japan and Singapore who have certified themselves to be in compliance with a level of this standard as evidence for their existing and potential future customers of their ability to resist and mitigate the possibility of attacks by harmful or fraudulent individuals and

organizations.

For those organizations that chose to use the ANSI/NASPO security assurance standard as a contractual specification or to show voluntary compliance, the conformity assessment services of NASPO have been available for verification of compliance and certification since 2003.

The examples given above provide an indication of how and in what way the existing ANSI/NASPO security assurance standard is being used by government agencies, large multinational corporations and smaller security solution producer/provider organizations in various parts of the world. If the pattern of use of the proposed ISO MSS follows the examples given above, it can be expected that it will be used as both a guidance document, contractual specification and regulatory specification. The primary intent, however, is that it be used as a contractual specification.

A.2.3 Need for an MSS

a) What is the need? Does the need exist at a local, national, regional or global level? Does the need apply to developing countries? Does it apply to developed countries? What is the added value of having an ISO document (e.g. facilitating communication between organizations in different countries)?

THE NEED?

With the advent of the terrorist attacks of September 11, 2001 it was no longer acceptable, anywhere in the world, for any organization involved in security to maintain the pretense of an ability to assure security without independent verification of their claimed ability by an accredited conformity assessor.

This attitude towards the possibility of “security pretenders” quickly spilled over into efforts ongoing worldwide to stem the rising tide of fraud in all of its forms and manifestations from the counterfeiting of products and prescription drugs to the theft of personal identity. Together, these attitudes gave rise to the need to :-

- set security assurance standards and
- develop methods of conformity assessment

to enable bona fide security organizations to differentiate themselves from the pretenders and demonstrate in an objective manner their ability to resist, to an acceptable degree, the attacks of harmful and fraudulent individuals and organizations.

In North America, this need was satisfied by :-

- the formation of NASPO
- creation of the ANSI/NASPO security assurance standard and
- creation of the NASPO conformity assessment methodology and certification service.

Demand for this service continues to grow in North America and elsewhere in the world as evidenced by the certifications, mentioned above, that have taken place in Europe and Asia. A similar experience has been found in Europe where demand for verified compliance with a similar standard for security printers, the CEN CWA 14641/Intergraf standard, has also experienced increased international demand.

DOES THE NEED EXIST AT A LOCAL, NATIONAL, REGIONAL or GLOBAL LEVEL?

The need exists at all of these levels because fraudulent and harmful acts occur and impact all of these levels. As well, the need exists at all of these levels because security focused organizations exist at all of these levels. This assertion is supported by the fact that security focused organizations exist in all of the developed and many developing nations and now, arguably, are large enough in numbers and economic activity to form a global industry. It is from within this global industry of security focused organizations that end users (relying

parties) select the most effective solution for their particular fraud countermeasure and control purpose. For this reason, a user based in Europe, for example, must know in advance of making a commitment to a product produced in Asia that the Asian organization is able to assure security to the standard required by the European end user in spite of constraints that might be imposed by national laws, regulations, social norms and traditions applicable to the Asian supplier. We believe that this example demonstrates the need for an internationally valid standard and method of conformity assessment.

DOES THE NEED APPLY TO DEVELOPING COUNTRIES?
We believe it does because many developing countries are severe victims of fraud particularly prescription drug related fraud. For this reason, there is need in those countries to know that any investment they make in security to combat fraud is coming from a bona fide source that meets or exceeds an acceptable security assurance standard. The existence of a recognized international security assurance standard will enable developing countries to specify their need and be sure about suppliers and providers.

DOES (THE NEED) APPLY TO DEVELOPED COUNTRIES?
Yes for the reasons given above under THE NEED.

WHAT IS THE ADDED VALUE OF HAVING AN ISO DOCUMENT?
Security assurance involves a multitude of risks including identification and management of risks that are related to the human resources (personnel) of an organization. This is a very sensitive area that must avoid violation of applicable human rights, invasion of privacy laws, personnel policy norms, social norms and national or cultural traditions. In the case of compliance with the ANSI/NASPO security assurance standard, experience has shown that in some countries these constraints make it difficult to perform adequate due diligence on personnel employed. As a result, relying parties remain uncertain about the security risk they are taking in contracting with foreign organizations. An ISO document will solve this problem by revealing to a relying party what due diligence can and cannot be carried out under the prevailing laws, regulations and traditions applicable in each ISO member country. This, we believe, represents a major added value of an ISO document.

b) Does the need exist for a number of sectors and is thus generic? If so, which ones? Does the need exist for small, medium or large organizations?

DOES THE NEED EXIST FOR A NUMBER OF SECTORS AND IS (IT) THUS GENERIC? IF SO WHICH ONES?
It is anticipated that there may be a need for sector specific versions of an otherwise generic MSS. For example, NEN has recently proposed a NWI for ISO/TC 130 to create a similar security assurance standard applicable to the security printing industry. This NWI, if approved, could be treated as a sector specific annex of the more generic MSS proposed in this NWIP. Another example concerns the unique security assurance requirements of organizations who are the custodians of personally identifiable information (PII). Authorities who issue identity documents are an example of such organizations. They also have unique security assurance requirements related to members of staff coming into contact with members of the public who may be harmful and fraudulent. Either way, it is clear that annexes of sector specific security assurance requirements may be required to render an otherwise generic MSS applicable to unique sector and/or operational requirements. It is not anticipated that the annexes will extend to individual versions for each sector (separate industry) as defined by ISO.

DOES THE NEED EXIST FOR SMALL, MEDIUM OR LARGE ORGANIZATIONS?
The need exists for all sizes of organization because, on a global scale, organizations who must maintain confidence and trust in products, information and services includes :-

- major government agencies,
- large multinational corporations,

- medium size security providers and
- small entrepreneurial organizations striving to develop innovative products.

All, within this chain or network, must be concerned with the assurance of security. All, we believe, will benefit from the use of an internationally recognized security assurance standard.

c) Is the need important? Will the need continue? If yes, will the target date of completion for the proposed MSS satisfy this need? Are viable alternatives identified?

IS THE NEED IMPORTANT?

Security Assurance has become a paramount issue to both public and private sector organizations throughout the world. The protection of persons, consumers, goods, services, and intellectual property from fraudulent activity is a critical problem in the economies of the world. The development of an internationally recognized security assurance standard can counter the efforts of this fraudulent activity and promote the development of trusted suppliers and supply chains, thus enhancing global trade.

The security industry, we must emphasize, is unusual because it often places a higher priority on security assurance than quality or other forms of assurance. Regardless of investments made by a security organization in quality or any other form of assurance, if security cannot be assured their security products or services are likely to be declared of little or no value by the world of end users (relying parties). For example, if a security technology or solution is, or becomes commercially available (meaning anyone can obtain it), it has no security value because fraudsters can obtain it and use it to their advantage. To be of security value a technology or solution must be protected on a routine and on going basis from unauthorized access and use and a relying party (the end user) must be certain of this otherwise the security value is gone. This is the essence of security assurance. For this reason, the security assurance MSS proposed by this NWIP is of paramount importance to the global economy.

In their recent deliberations, participants and observers in ISO/PC 246 – Performance Criteria for Authentication Solutions, were cogent in their emphasis of the importance of including security assurance requirements in the performance criteria applicable to authentication solution providers. Their reasons for inclusion were identical to the example given in the preceding paragraph. The matter was referred to the contiguous initial meeting of ISO/TC 247 – Fraud Countermeasures and controls. At that meeting the importance of security assurance requirements was brought forward from ISO/PC 246 and combined with a proposal from the US delegation to consider development of a NWIP for the MSS that is the subject of this NWIP. The outcome of ISO/TC 247 deliberations culminated in a resolution for ANSI to prepare this NWIP and submit it within a 3 week period for formal review and ballot by all ISO/TC 247 “P” members. The urgency attached to the preparation of this NWIP by all participants and observers present at the ISO/TC 247 meeting, is a measure of the importance attached to this MSS by those subject matter experts.

WILL THE NEED CONTINUE?

Yes, it will continue because a security assurance standard is fundamental to fraud countermeasures and controls. The need for security assurance will always exist. The need for an international standard is long overdue for all of the reasons given above.

IF YES, WILL THE TARGET DATE OF COMPLETION FOR THE PROPOSED MSS SATISFY THIS NEED?

The date is not ideal but it is conservative given the maturity that exists in the ANSI/NASPO standard and conformity assessment methodology that this NWIP has proposed as the basis of the ISO MSS. We believe that the international community of potential users would welcome an early, expedited release of the proposed MSS

d) Describe how the need and importance were determined. List the affected parties consulted

and the major geographical or economical regions in which they are located.

DESCRIBE HOW THE NEED AND IMPORTANCE WERE DETERMINED
In North America, the need was determined initially by the logic expounded above and the formation of NASPO and its' founding members. The founding members of NASPO were either security technology developers, solution providers or end users. In 2005 NASPO was encouraged to elevate the private standard it had created, to national level through ANSI accreditation of NASPO as an American national standards development organization. In North America, it was this process that confirmed the need for the ANSI/NASPO security assurance standard. In Europe, a similar process under the auspices of CEN, confirmed the need for a similar standard applicable to the security printing industry. The result in Europe was the CEN CWA 14641 – Security Management System for Security Printing. As mentioned earlier, this CEN CWA is now the subject of a proposed NWIP under consideration by ISO/TC 130.

The broader international need and importance were determined by :-

- observation of the demand by multinational corporations for certification of their suppliers outside of North America,
- observation of the demand by government agencies for certification of foreign suppliers and
- voluntary demand by security solution providers outside of North America convinced of the importance of demonstrating their high security assurance standards by compliance with a recognized high standard.

CEN in Europe, we believe, claim to have made similar observations that have lead them to the same conclusion of need and importance.

LIST THE AFFECTED PARTIES CONSULTED AND THE MAJOR GEOGRAPHICAL OR ECONOMIC REGIONS IN WHICH THEY ARE LOCATED.
As a result of the essential requirements of ANSI for the development of American national standards, all of the affected parties listed above in Section A.2.2 items 1-6 were consulted to confirm the need and importance of the ANSI/NASPO security assurance standard. A similar list of affected parties were consulted as part of the process used to confirm the need for and importance of the security management system workshop agreement for security printers developed by CEN. Outside of the USA consultation has taken place with :-

- ASIS International who certify protection professionals worldwide
- Brady Corporation in Singapore
- TUV Rheinland Group located in Germany, USA and Japan
- ISO/TC 247 and PC 246 "P" and "O" member nations :-
  - Brazil - South/ Latin America
  - Canada – North America
  - France - Europe
  - Germany – Europe
  - Israel – Middle East
  - Japan – Asia
  - Netherlands – Europe
  - South Korea – Asia
  - Switzerland – Europe
  - United Kingdom – Europe

e) Is there known or expected support for the proposed MSS? List those bodies that have indicated support. Is there known or expected opposition to the proposed MSS? List those bodies that have indicated opposition.

IS THERE KNOWN OR EXPECTED SUPPORT FOR THE PROPOSED MSS?
Yes there is both known and expected support.

BODIES THAT HAVE INDICATED SUPPORT INCLUDE ;

- American Bank Note Company
- ASIS International
- Bristol Myers Squibb
- Datacard Corporation
- Honeywell
- Intel Corporation
- International Authentication Association
- ITW Covid
- JDSU Authentication Solutions
- Polyonics Inc.
- TUV Rheinland Group
- US Customs & Border Patrol
- US Document Security Alliance
- US National Institute of Science & Technology (NIST)

ISO/TC 247 and PC 246 delegates from :-

- Brazil - South/ Latin America
- Canada – North America
- France - Europe
- Germany – Europe
- Japan – Asia
- Netherlands – Europe
- South Korea – Asia
- Switzerland – Europe
- United Kingdom – Europe
- USA – North America

IS THERE KNOWN OR EXPECTED OPPOSITION TO THE PROPOSED MSS?

No, to date, no bodies have indicated opposition.

A.2.4 Sector-specific MSS proposals

a) Is the MSS for a single specific sector?

No, it is expected to be globally applicable to all sectors that are impacted by fraud.

b) Will the MSS reference or incorporate an existing, non-industry-specific ISO MSS (e.g. from the ISO 9000 series of quality management standards)? If yes, will the development of the MSS conform to the ISOIIEC Sector Policy (see 6.8.2 of ISO/IEC Directives, Part 2, 2001), and any other relevant policy and guidance procedures (e.g. those that may be made available by a relevant ISO technical committee)?

WILL THE MSS REFERENCE OR INCORPORATE AN EXISTING, NON-INDUSTRY-SPECIFIC ISO MSS (E.G. FROM THE ISO 9000 SERIES OF QUALITY MANAGEMENT STANDARDS)?

Yes. It will make normative reference to part or all of the ISO/IEC 27000 series, 28000 series, and any other MSS that is relevant to operational security, risk management or risk assessment.

WILL THE DEVELOPMENT OF THE MSS CONFORM TO THE ISOIIEC SECTOR POLICY (SEE 6.8.2 OF ISO/IEC DIRECTIVES, PART 2, 2001), AND ANY OTHER RELEVANT POLICY AND GUIDANCE PROCEDURES (E.G. THOSE THAT MAY BE MADE

AVAILABLE BY A RELEVANT ISO TECHNICAL COMMITTEE)?

Yes. This policy defines the rules for making reference to ISO 9001:2000 when developing quality management system requirements for a particular product or industry/economic sector. It asks that requests for guidance on this sector policy etc, be submitted to the secretariat of ISO/TC 176. We assume that similar rules will apply when making reference to other ISO or ISO/IEC generic standards.

c) What steps have been taken to remove or minimize the need for particular sector-specific deviations from a generic MSS?

The generic security assurance MSS we are proposing will, in some way, need to address the unique requirements of specific industries and types of secure operation as and when they emerge. Our approach to removal is to exclude them from the generic body of the MSS document and to include each of them in the form of an annex attached to the main body. At this time we anticipate the need to include, in this way, unique requirements associated with the security printing industry and identity document issuing operations.

A.2.5 Value of an MSS

The primary value of a security assurance MSS is the creation of barriers to fraudulent actions that result in both social consequences and economic losses. Currently, global economies are under substantial attack from fraudulent activities. These activities cost citizens and businesses, within these economies, hundreds of billions of Euros/Dollars annually. In addition, these fraudulent activities can result in loss of life and serious injury of our citizens through adulterated or counterfeit products, and fund criminal activities that range from the smuggling of illicit products and drugs to human trafficking. Broad implementation of an internationally recognized security assurance standard will begin to build the necessary framework for the protection of legitimate products and critical services.

A.2.5.1 Value to an organization implementing the MSS

a) What are the expected benefits and costs to organizations, differentiated for small, medium and large organizations if applicable?

Benefits

Regardless of size, an organization seeking a security product or service must be able to unambiguously specify the level of security assurance it requires and the producer/provider seeking to sell its solution or services must then convince the buyer that it is able to comply. To this end, the proposed security assurance MSS will enable users and buyers to unambiguously specify their requirements for security assurance and producer/providers to supply evidence of their ability to comply.

More specifically, a significant benefit of implementation for all sizes of organization is the knowledge gained by a party concerning the level of security risk it will be taking in using the products or services of that organization. This risk has nothing to do with the financial or quality related risks of doing business. It concerns the degree to which the relying party is convinced that the organization, through the use of security infrastructure, systems, procedures and security risk management methods required by this MSS, is able to prevent, detect and control acts and threats posed by the perpetrators of fraud. Those acts and threats, if they are not resisted, could potentially eliminate or substantially degrade the value of security products or services offered by an organization.

As outlined above, the proposed MSS will provide this knowledge through clear and unambiguous definition of what is required by a relying party. This, together with the methods of verification of compliance can then be used by the producer/provider to convince the

relying party either directly or by independent conformity assessment of compliance with the MSS.

In a number of cases, organizations claim to have gained business as a direct result of implementation and compliance with the ANSI/NASPO security assurance standard. Others claim that their compliance with the standard has made them significantly more confident about their ability to assure security and some go further and claim that compliance has removed a competitive disadvantage and gained them increased business opportunities.

Organizations lacking the skills and resources to adequately evaluate the security assurance of an organization would be able to specify security levels for the providers of their products and services. By using compliant suppliers it removes significant time and costs from the procurement process by eliminating the necessity to individually audit each organization. It also provides a very cost effective means for organizations to meet security compliance requirements by providing a single internationally recognized standard versus compliance with multiple industry/organizational specific standards.

Costs

The cost of implementation of the proposed MSS must bear in mind the reality that security costs money and the higher the security the more it tends to cost. Needless to say, there is an extra cost to providing security assurance just as there is an extra cost to quality assurance. The extra cost involves the special infrastructure, systems, procedures and management that must be implemented to assure a level of security. These costs exist regardless of implementation of the proposed MSS. That said, the extra cost of implementing the MSS will be :-

a) the time and talent taken to study the specific requirements of the MSS,
b) developing and assembling evidence of compliance,
c) closing any gaps in security that are required to satisfy the requirements specified and
d) in the event of a requirement for certification by a relying party, payment of any fees that are involved to a certification body for assessment of conformity.

For those organizations that have existing security infrastructure, systems, procedures and security management, the cost will likely be confined to items a, b and d and a very small c. The total of these costs are not expected to be significant when compared to the investment already made in security infrastructure and systems etc. For small organizations the reverse is not uncommon. For those organizations, the difficulty and cost of implementation maybe prohibitive. Arguably, organizations who cannot bear the extra costs of security assurance should not attempt it unless a way can be found to avoid the risks in a manner that is acceptable to relying parties. For the majority of members of this industry the costs are expected to fall within these extremes. For the majority, the cost and difficulty will not be prohibitive but significant enough that a business case may need to be made to weigh the costs and benefits in advance of implementation.

Implementation and compliance with the Class II mid-level of security assurance found in the ANSI/NASPO security assurance standard, for a single site employing 50-100 persons, typically takes 6-8 months and involves a team of 6-8 people working part time. Based upon this duration and level of effort the cost of completing items a) and b) is in the region of US$65,000 to US$95,000. The cost of item c) is the most variable of the items and totally dependent upon the nature and extent of gaps to be closed. The cost of item d) for NASPO Class II certification can range from US$6,500 to US$11,500.

Comparable costs for Implementation and compliance with the ANSI/NASPO Class I high-level of security assurance is typically 50-60% greater than Class II for items a) and b) with item d) ranging from US$10,500 to US$16,500. For the ANSI/NASPO Class III basic level, the comparable costs for a) and b) are 30-40% less than Class II with the cost of d) ranging from US$5,500 to US$9,500.

b) Describe how the benefits and the costs were determined. Provide available information on geographic or economic focus, industry sector and size of the organization. Provide information on the sources consulted and their basis (e.g. proven practices), premises, assumptions and conditions (e.g. speculative or theoretical), and other pertinent information.

DESCRIBE HOW THE BENEFITS AND THE COSTS WERE DETERMINED.

The benefits were determined by a consensus of the members of NASPO, a market survey commissioned by NASPO and the body formed to reach American national consensus on the ANSI/NASPO security assurance standard. The cost figures are based upon eight years of experience within NASPO of working with organizations on the implementation and certification to the ANSI/NASPO standard. The ANSI/NASPO Class II level of security assurance was used as the reference because the majority of implementations and certifications have fallen into that Class.

c) Will the MSS allow an organization competitively to add to, differentiate or encourage innovation of its management system beyond the standard?

Yes. Although the proposed MSS represents minimum standards, at three or more levels of assurance, the standard caters for betterment by offering a set of what it terms “risk reduction enhancements”. The latter are a set of electives that a more security conscious organization can elect to implement to better meet the needs of its’ relying parties. As well, the MSS proposed in most cases is not wholly prescriptive in how it expects a requirement to be implemented. This leaves sufficient scope for security assurance innovation including how best to treat vulnerabilities that are exploited by the threats.

d) If the intended use is for contractual or regulatory purposes, what are the potential methods to demonstrate conformance (e.g. first party, second party or third party)? Does the MSS enable organizations to be flexible in choosing the method of demonstrating conformance, and to accommodate for changes in its operations, management, physical locations and equipment?

The major intended use is for contractual or regulatory purposes. To this end, the preferred method to demonstrate conformance is via the third party method carried out either by the MSS authority itself or via accreditation of independent certification bodies by the MSS authority. In some cases relying parties may be content to accept first party evidence of compliance in order to avoid the cost of third party audits that may cause an increase in the cost of the product or service and/or the effort and hence cost of their own second party audit.

DOES THE MSS ENABLE ORGANIZATIONS TO BE FLEXIBLE IN CHOOSING THE METHOD OF DEMONSTRATING CONFORMANCE,

In the case of this MSS it is expected that the choice will be driven more by the relying party than the security producer/provider. The proposed MSS is not expected to dictate the method (in terms of first, second or third party) to be used to demonstrate conformance but neither is it expected, per se, to enable flexibility of choice. However, there is expected to be nothing contained in the MSS that will preclude an organization from self asserting conformity and furnishing the same evidence (it would expect to provide to a third party auditor) directly to a relying party. It is then up to the relying party to accept or reject evidence presented in this way. Given the possibility of demonstrating conformance by self assertion it is arguable that flexibility is enabled.

DOES THE MSS ACCOMMODATE FOR CHANGES IN ITS OPERATIONS, MANAGEMENT, PHYSICAL LOCATIONS AND EQUIPMENT?

Yes. Production operations are in no way constrained by this MSS provided that the changes made do not remove or degrade the security measures that may be a necessary part of the production operation. For example, for security reasons it is important to know if product or materials, having security value, are missing. The internal track and trace system, that provides this intelligence, must continue to function properly regardless of changes in production methods or operations. Security assurance operates on the principle that operations, management, physical locations and equipment can all be changed provided that in so doing :-

a) no vulnerabilities are created that are not covered by risk assessment and adequate risk reduction,
b) no security procedures are abandoned or responsibility abdicated unless they are rendered unnecessary or obsolete by the nature of the changes made,
c) those responsible for security management within the organization have carried out an assessment of impact on security assurance and if any are found that appropriate corrective action is taken.

e) If third-party registration/certification is a potential option, what are the anticipated benefits and costs to the organization? Will the MSS facilitate joint audits with other management system standards or promote parallel assessments?

Third-party registration/certification is a potential option. The anticipated benefit of third party registration/certification for the relying party is that it relieves that party from carrying out its own assessment of conformity. The relief may simply be a matter of convenience or a lack of resources or know how to do it. For the relied upon party there may be no relative advantage compared to second party assessment. The benefit of third party assessment is that it removes the possibility of bias towards others that might be present in a second party assessment and the self serving/lack of objectivity stigma that tends to be associated with self assessment (first party assessment). The anticipated costs of third party registration/certification are given above under A 2.5.1 a).

We anticipate that this MSS will be audited in conjunction with other existing ISO Standards. In particular we would expect the proposed MSS to be audited in conjunction with ISO 2700 series and 28000 series standards to create a security assurance package of compliance. By auditing as a suite of standards it provides a broad spectrum approach to security assurance that is cost effective for the end user.

A.2.5.2 Value to other affected parties

a) What are the expected benefits and costs to other affected parties (including developing countries)?

The use of security assurance practices and procedures can impact people at every level in an organization. Discipline is involved. Background checks are carried out. There are more rules to follow and serious consequences exist if breaking those rules causes a breach of security. Security assurance also places some abnormal expectations on employees. All employees are expected to be the ears and eyes of the organization, constantly on the look out for breaches and willing to report the misconduct of even close working associates. Some, who are new to a security culture, often find it objectionable and leave. Others thrive on it knowing that they are working within a secure environment it provides them a greater sense of security in the workplace. The social and psychological affects of security assurance will impact some employees negatively and be an opportunity for others to thrive. On balance we believe the net impact and hence cost to employees to be positive. The benefit to this affected party of people, of this MSS, is continued employment. In today's world, if their

employer is unable to assure security to some standard, the employer may be unable to secure the contracts that will keep them employed.

The main benefit of an international security assurance MSS is that a standard is set that has multiple uses to a multitude of individuals and organizations many of whom are effected by the mere existence of the standard. They are affected because a standard now exists that can be used :-

- as a reference or bench mark against which to judge the adequacy of their own or another security assurance standard,
- as part of an overall fraud countermeasure and control strategy
- as an internal guideline
- as the basis of a security assurance training course
- as a means of learning the fundamentals of what security assurance means and yields,
- to make the case to require security assurance,
- as a ready made requirement specification that enables the level required to be matched to the consequences of failure to counter and control credible threats posed by harmful and fraudulent individuals and organizations waiting to exploit vulnerabilities.

In most cases the cost of using the standard, as outlined above, will be no more that the purchase price of the standard itself. For developing countries, consideration could be given to waiving or reducing the purchase price.

One of the primary goals of this standard is to mitigate the effects of fraud in products and services. Unfortunately developing nations may be the most affected by this fraudulent activity. They are often the victims of counterfeit pharmaceuticals, forged documents, identity fraud, counterfeit parts, and corrupt product/service providers. The development of this MSS is supportive of the efforts to curtail these activities in developing nations. The establishment of trusted sources supplying these developing nations may provide the means to support economic growth and combat the social consequences of fraud.

b) Describe how the benefits and the costs were determined. Provide any information regarding the affected parties indicated.

The benefits were determined by discussions among the delegates of ISO/PC 246, ISO/TC 247 and members of the North American Security Products Organization (NASPO) – an ANSI accredited American national standards development organization.

c) What will be the expected value to society?

The practical contribution made to society by security assurance is that it assures and in some cases significantly increases resistant to fraudulent acts such as:-

- false issuance of primary identity and travel documents caused by internal fraud and malfeasance,
- unauthorized access to security sensitive materials, know how and information that are increasingly used to authenticate products and combat counterfeiting, falsification and intellectual property rights
- interception of security sensitive goods that enable fraudulent mimics or simulations to be made of security devices used as proof of compliance, payment (e.g. tax stamps), access permission, authenticity,
- avoidance of government revenue taxes,
- exploitation of weak links in supply networks such as prescription drugs, legacy parts used in critical infrastructure systems, aircraft and auto parts etc. that enable non

compliant substandard parts, items and materials to be introduced as genuine into the supply chain,
- willful exportation of goods that violate fair trade rules,
- unauthorized access to information that criminal elements use to enable them to plan, initiate and optimize harmful acts, for example, hijacking, physical intrusion, confidence tricking, computer hacking etc.

In so doing the proposed security assurance MSS is contributing to the prevention, detection and control of identity, product, critical component, document, financial instrument, healthcare etc. related fraud for the benefit of society in general.

A.2.6 Risk of trade barriers

a) How would the MSS facilitate or impact global trade? Could the MSS create or prevent a technical barrier to trade?

HOW WOULD THE MSS FACILITATE ……..GLOBAL TRADE?
Custom organizations worldwide are fighting to prevent the importation of illicit goods into their countries. The challenge has now progressed to the point where it is becoming necessary to avoid the overwhelming task, of inspection at ports of entry, by relying on assurance of authenticity back through the supply network such that prior to exportation it is known that no trade laws will be violated. The proposed security assurance MSS can be used to both establish and verify the network of trust that relying customs parties require to accept goods for importation at the point of exportation. In this area of world trade, the proposed security assurance MSS may be the enabler of a much in demand new form of customs inspection. Discussion of the latter and a proposal for a specific NWIP to cover it was made by the US delegation at the recent ISO/TC 247 based upon needs identified by the US Customs and Border Patrol (US CBP) agency.

HOW WOULD THE MSS ……IMPACT GLOBAL TRADE?
Security assurance is germane to deterring, detecting, controlling and countering all forms of product, identity and service fraud. Although indirect and somewhat in the background, the proposed MSS, if properly and extensively used, is expected to contribute to reduction in the incidence and motivation to gain unfairly from the trading of fraudulent products, services and identities. In short we expect a small positive impact generally. If effort is focused and targeted at specific problem areas such as the above customs problem and international trading in illicit prescription drugs, especially in third world countries, the positive impact may be significant.

In addition, this MSS will have the ability to build trusted supplier networks and supply chains throughout the world. This will enable an international recognition of security compliant organizations by those organization seeking the products and services of those global producers. The overall effect is to enable greater trust in global trade in products and services of value.

Could the MSS create or prevent a technical barrier to trade?
The proposed MSS is aimed at assuring the efficacy of security products and services. It neither creates or prevents a technical barrier to trade. Assurance is the process of providing relying parties with confidence and trust in security producer/providers who are at arms length and not under control of the relying party.

b) Could the MSS create or prevent a technical barrier to trade for small, medium or large organizations?
No, for the reasons expounded in a) above.

c) Could the MSS create or prevent a technical barrier to trade for developing or developed

countries?
No, for the reasons expounded in a) above.

d) If the proposed MSS is intended to be used in government regulations, is it likely to add to, duplicate, replace, enhance or support existing governmental regulations?
Governments of most, if not all, ISO member nations are expected to have already established, and be making use of, some form of security assurance standard in their regulations. For example in the United States, government has established the National Industrial Security Program and Operating Manual (NISPOM)[1] to regulate government contractors, especially defense contractors. The NISPOM is a highly prescriptive set of security assurance rules that contractors are obligated to follow. Similar prescriptive security assurance regulations are known to exist in other countries but most are not made publicly available for security reasons. In the United States, a number of government agencies are making use of the ANSI/NASPO security assurance standard as an alternative to the NISPOM. In this sense, it has replaced the NISPOM but not duplicated it. In some cases government agencies use it as a contractual obligation, in others it is a recommended guideline. In all cases it is supporting and arguably enhancing existing government regulation. We expect that the pattern of use by regulating bodies elsewhere in the world could follow that of the United States.

A.2.7 Risk of incompatibility, redundancy and proliferation

a) Is there potential overlap or conflict with other existing or planned ISO or non-ISO international standards, or those at the national or regional level? Are there other public or private actions, guidance, requirements and regulations that seek to address the identified need, such as technical papers, proven practices, academic or professional studies, or any other body of knowledge?

The only potential overlap we are aware of, concerns an interest, on the part of the Netherlands standards body NEN, to establish an MSS specific to the security printing industry.

We fully expect that there are other similar efforts in the world at a national, regional, or industry level. We would also acknowledge that there has been technical papers and academic or professional studies conducted. We do not believe that those efforts overlap or are in conflict with this MSS. On the contrary, we believe that the concepts expressed in this MSS are consistent with those efforts. We are not aware of other ISO or non-ISO initiatives or other private or public actions that involve potential overlap or conflict other than the proposal to ISO TC 130 mentioned above.

b) Is the MSS or the related conformity assessment activities (e.g. audits, certifications) likely to add to, replace all or parts of, harmonize and simplify, duplicate or repeat, conflict with, or detract from the existing activities identified above? What steps are being considered to ensure compatibility, resolve conflict or avoid duplication?
Discussions are ongoing between the Secretariat's of ISO/IEC JTC-1 and ISO/TC 247-Fraud Countermeasures and controls and other technical committees to determine if any overlap and conflict exists and, if so, how they might be resolved. As indicated in this NWIP and section A.2.1 g) the MSS proposed by this NWIP is planned to cater for specifications of the unique security assurance requirements of specific industries, economic sectors and extraordinary operations with the addition of annexed sections to the generic body or versions to create a family of security assurance standards. Further discuss on this matter can be found in section A.2.3 b) above. We also view the standards developed under ISO

[1] National Industrial Security Program Operating Manual (NISPOM). US Department of Defense document No. DoD 5220.22-M, 1995 available at http://cryptome.org/nispom/nispom.htm

27000 and ISO 28000 to be complimentary to the proposed MSS and would seek harmonization with these MSS's.

c) Is the proposed MSS likely to promote or stem proliferation of MSSs at the national or regional level, or by industry sectors?
The present NWIP before ISO/TC 247 is to create an MSS, that is filling a vacuum for a broad based security assurance MSS. This MSS has the potential to grow into a family of industry sector and operations specific security assurance requirements. The mere existence of this ISO standard may well stem the necessity at national, regional and industry sector levels to create their own home grown versions provided that the ISO, as planned, adequately addresses the unique needs of this hierarchy. It is our hope and belief that the new security assurance MSS proposed will attract nations, regions and sector industries with unique requirements to standardize them in the form of additions to the proposed ISO MSS framework rather than realize them in the form of independent standalone standards that relying parties may not recognize. The attraction we have annunciated above, in effect, stems the proliferation of security assurance standards. We do not believe that the proposed MSS will cause (promote) proliferation of security assurance standards. We see nothing that would motive this to happen.

A.2.8 Other risk factors

Have any other risks been identified (e.g. timeliness or unintended consequences to a specific business)?
Yes. Unintended consequences to specific businesses have been addressed. The risk here is that a requirement to comply with a high level of security assurance may become a business issue for some organizations.