ANSI/NASPO-SA-2008

# Security Assurance Standards

Important Notification: This document remains the sole property of the North American Security Products Organization (NASPO). Any unauthorized use of this document or any aspect of its prescribed procedures is strictly prohibited without authorization.
Requests for authorization should be directed to:
NASPO: www.naspo.info

© NASPO 2008 All right reserved

**1425 K Street, NW, Washington, D.C. 20005, U.S.A.**
www.naspo.info

# Executive Summary

This document identifies and defines risks that a secure operation must manage and the degree to which those risks must be managed to be certified by NASPO as a Class I, II or III secure operation. The risks defined result from actions that individuals, syndicates, cartels and other unlawful individuals or third party organizations with serious criminal intent to acquire, circumvent, mimic or subvert physical security items, technologies, services or information may perform in their intent to commit fraud.

To obtain ANSI/NASPO Certification, organizations must demonstrate a sharp awareness of possible fraudulent actions, recognize that they pose a threat to the value of their security items, implement countermeasures aimed at preventing them, put plans in place and be prepared to use them to mitigate their effects in the event that fraudulent acts occur.

The contents which follow enable a secure operation, who know their customer or end user needs for security assurance, to classify and officially certify themselves, through a NASPO or commercial audit, with the ability to deliver either a high, medium or basic level of security assurance.

Conversely, customers or end users who know their need for security assurance can use the contents to specify their requirements broadly, by selecting a Class of Certification, or more specifically by choosing areas of risk and methods that suppliers and/or internal groups must use to reduce those risks. As well, end users who believe that the best method of protecting a security technology is to form a partnership of shared risk management responsibility with the supplier, can use the contents as a reference to ensure that risks are covered adequately by both sides of the partnership.

Either way, NASPO was faced with the challenge of conveying, in this document, a clear understanding of what is meant by "*security assurance*" combined with the creation of an objective system for specifying, standardizing and verifying the degree to which it is delivered.

This update to the ANSI/NASPO Security Assurance Standard was achieved by a process of consensus (APPENDIX B ) that is manifested in a revised set of risk management requirements that represent best practices found in recognized high security (NASPO Class I), medium security (NASPO Class II) and basic security (NASPO Class III) operations. Credits are awarded by NASPO auditors for the verified existence and use of these best practices which NASPO term Certification Criteria. The Certification Criteria represent specific risk reduction infrastructure, systems and techniques that assure security. They are identified in Section 6 and defined in Appendix A. The areas of risk they address are detailed in Section 5. The Classes of NASPO Certification are defined in Section 4.

Organizations seeking ANSI/NASPO security assurance certification can determine their readiness by carrying out a self assessment of compliance. To be ready, it is important that applicants come close to satisfying all of the mandatory certification criteria specified for each Class in Section 6 and any risk reduction "enhancements" they have chosen. Overall, certification will depend on NASPO auditors being satisfied that the risk management objectives defined in Section 6 are actually being met. This means that the risk reduction infrastructure, systems, and techniques etc must be properly implemented, used and not just exist.

Verification that the required Class of security assurance is being delivered will be the responsibility of NASPO auditors. An outline of the audit process and the methods of verification that will be used, are given in Section 7. Background to the development of these consensus standards and legal matters are given in APPENDIX B .

NASPO welcomes comment and feedback on the content of this document. Please address your input to NASPO at nnsc@naspo.info

# Table of Contents

**The balance of this page is intentionally left blank.**

# 1.0 Introduction & Purpose

The purpose of NASPO Certification is to demonstrate that the security value of technologies, services and products offered and used by NASPO Certified Organizations are unlikely to be undermined either by fraudulent acts or negligence.

To obtain NASPO Certification, organizations must demonstrate a sharp awareness of possible fraudulent actions, recognize that they pose a threat to the value of their security products, implement countermeasures aimed at preventing them, put plans in place and be prepared to use them to mitigate their effects in the event that fraudulent acts occur.

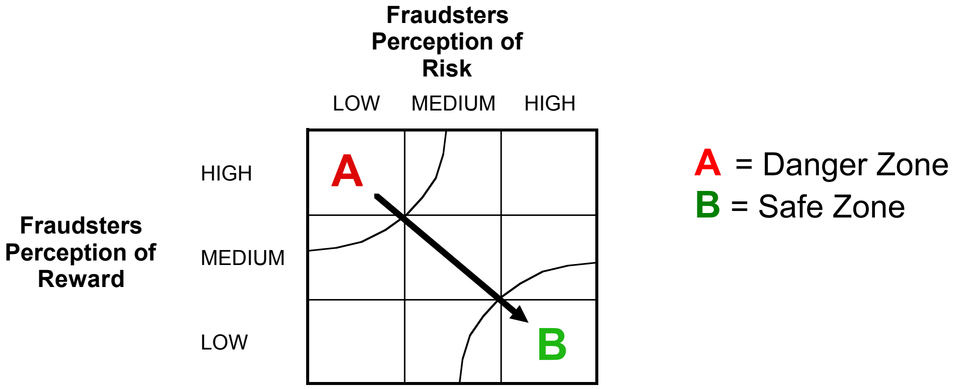
To this end, the contents of this document specify **Standards of Security Assurance** that must be met by organizations who apply for ANSI/NASPO Class I, II or III Certification. The specifications include:-

- areas of risk that organizations must manage
- the distinctions between Class I, II and III Certification
- objectives that must be satisfied by the risk reduction methods that are used
- types of risk reduction infrastructure, systems and procedures that must be implemented to comply with Class I, II or III certification
- the procedure that NASPO auditors will follow to verify that the standard of security assurance claimed by an organization is in fact being met.

The purpose of this document is to identify and define risks that a security products producer or consumer must manage and the degree to which those risks must be managed in order to be certified by NASPO as a Class I, II or III organization. The risks defined are actions that individuals, syndicates, cartels and other unlawful third party organizations with serious criminal intent to defeat a given security technology might take to circumvent, mimic or subvert security products or information.

## 2.0 Security Value of Products & Services

The goal of most security technology, products and services is to prevent fraud by moving perception of risk and reward from the top left hand corner (the high reward/low risk zone) of the matrix shown below, to the bottom right (low reward/high risk zone) and having done that, to keep it there permanently. The function performed is that of a deterrent.


Fraudsters Perception of Risk
LOW
MEDIUM
HIGH
Fraudsters Perception of Reward
HIGH
MEDIUM
LOW
A
B
A = Danger Zone
B = Safe Zone

Other security products enable fraud to be detected or perform an authentication or track and trace function and some combine these functions with the power to deter. Track & trace products enable their users to detect fakes and furnish forensic evidence.

Products and services that are available to perform these functions we refer to as Security End Items (SEI's). Some are complete systems (or packages) such as passport documents, printers and readers. Some are components that require integration such as special inks, taggants, laminates and security devices. The goal of NASPO is to certify that the makers and suppliers of SEI's are bona-fide, observe a security industry code of practice and properly manage security risks to the benefit of themselves, their customers, end-users and the public at large.

## 3.0 Scope

### 3.1 Risk Management Requirements

The requirements set forth in this document apply only to the management (control) of risks that have the potential to either reduce or eliminate the value of a security technology, product or service. The NASPO requirements **do not** address the intrinsic functional security value of a product or service, or in any way imply that a product or service is of security value. For these reasons, NASPO intends to rely on the market for security technology, products and services to evaluate properties such as, counterfeit resistance, tamper and alteration resistance, track and trace performance, authentication value and forensic evidence value etc.

The NASPO audit process will verify the nature and extent of security assurance practiced by a security producer or consumer and will determine if those practices are satisfactory and sufficient to warrant the class of certification requested by the organization.

### 3.2 Applicability of this Standard to End Users

The intent is that this standard will apply to those organizations who supply security technology and/or security products including organizations who supply products that feature a combination or integration of several security technologies. Users of security technologies or services may wish to apply these standards informally, to their own internal operations, to ensure that the security technologies or services they are using are protected inside their organizations.

## 4.0 Grades of Security Assurance

To an end-user, the value of a security product or service is a combination of the security functionality delivered, it's cost and the degree to which the maker protects it from all forms of fraudulent action such as :-

- theft of end product or critical components
- theft of critical (functionality) technical data
- theft of critical production know-how or equipment
- theft of forensic feature data

- posing as a bona fide customer
- theft of a raw material
- theft and disclosure of confidential and or personal information through deception and misrepresentation

When the security functionality of the product or service is effective, there is always the threat that individuals and criminal organizations will seriously attempt to defeat a given security barrier (caused by the security functionality) by taking one or more of the above fraudulent actions. Preventing or deterring these actions and mitigating their effects, if they happen, will be referred to as 'security assurance'. Verifying delivery of a class of security assurance will be the responsibility of NASPO auditors.

**4.1** **ANSI/NASPO Class I** certified organizations will be expected to deliver a very high level of security assurance by anticipating and effectively controlling all credible forms of fraudulent action to the point where attempts are eliminated because the barriers appear insurmountable and the chance of success appears to be non-existent. In the event that fraudulent acts do occur, organizations in Class I must be prepared to fully mitigate their effects.
The specific risk reduction requirements of Class I certification are defined in Section 6.0. To qualify for Class I certification, organizations must meet the objectives specified in each area of risk and comply with all Class I MANDATORY (M) certification criteria.

**4.2** **ANSI/NASPO Class II** certified organizations make security products or provide security services where the consequences of fraudulent action are less serious, but still must maintain a high level of security assurance. This level of assurance must be satisfactory and sufficient to protect the end-user's investment in the security product or service. In the event that fraudulent acts do occur, organizations in Class II must be prepared to substantially mitigate their effects.
The specific risk reduction requirements of Class II certification are defined in Section 6.0. To qualify for Class II Certification, organizations must meet the objectives specified in each area of risk and comply with all Class II MANDATORY (M) certification criteria.

**4.3** **ANSI/NASPO Class III** certified organizations (unlike Class I & II organizations) may not be focused on, and/or do not exclusively manufacture security products. Those products produced, generally suffer only from the threat of minimal economic loss and have limited consequences. As a result, full time Security Assurance may not be warranted but must be satisfactory and sufficient to protect the end-users investment in the security product. Organizations in Class III must have plans in place to mitigate the effects of fraudulent acts should they occur.
The specific risk reduction requirements of Class III certification are defined in Section 6.0. To qualify for Class III Certification, organizations must meet the objectives specified in each area of risk and comply with all Class III MANDATORY (M) certification criteria.

**4.4** **Risk Reduction Enhancements –** certification criteria shown with an **E** in the tables of Section 6 are referred to as Risk Reduction Enhancements (referred to later as "Enhancements"). Unless specifically called for by a NASPO auditor, customer or end user, there is no obligation on the part of a certification applicant to comply with any "Enhancements" unless a NASPO auditor notifies the Applicant in writing, at least 90 days in advance of an audit, that one or more will be required. Only in the event that an auditor identifies an unusual type of risk, that is not covered by any of the mandatory certification criteria, will such written notices be issued. In some cases, it is expected that certification applicants themselves will choose to enhance their risk reduction either to satisfy the requirement of a customer, to position for transition to a higher class of certification or to satisfy their own assessment of the need to go beyond the risk reduction that is mandatory in a specific class. Certification applicants who wish to include one or more "Enhancements" in a NASPO audit must notify the NASPO auditor 90 days in advance of a planned audit date otherwise the "Enhancements" will be overlooked. Verified compliance with all "Enhancements" included in a NASPO audit will be documented in the NASPO audit report.

**4.5 Exclusion of Requirements –** No mandatory requirements will ever be excluded from a NASPO audit. In the event that a mandatory requirement addresses a risk that does not exist, the auditor will note the fact after verifying that the risk is non existent in the case of the particular certification applicant. The NASPO audit report will then document the verified non existence and provide an assessment of impact, if any, on the award of a NASPO security assurance certificate.

Regardless of the class of certification, all NASPO certified organizations will be expected to deliver security assurance that addresses and controls the following areas of risk to a greater or lesser degree :-

(back to Table of Contents )

**The balance of this page is intentionally left blank.**

# 5.0 Risks to be Managed

## 5.1 Customer Related Risks

The ANSI/NASPO standard requires organizations to be vigilant to the possibility of orders for security products or services coming from fraudulent sources. To this end, NASPO auditors will expect to see that rigorous checks have been carried out to detect and manage purchase orders coming from fraudulent sources.

### 5.1.1 Fraudulent Re-Production

Organizations in the business of producing security products shall perform due diligence to avoid fraudulent reproduction of existing security products.

### 5.1.2 Delivery of Exact Quantities

As a part of security assurance, organizations shall use procedures and/or systems that enable customers to verify quantities delivered to an accuracy that can reasonably be expected, given the nature of the end product delivered.

## 5.2 Information Risks

General requirements for management of risks in this area are driven by the need to avoid disclosure and theft of information of potential strategic value to any individual or group interested in defeating or by-passing the protective features of a security technology, or selling such information to parties that are. In this area of risk, NASPO auditors will expect to find that no one without proper clearance and authority is provided with such information. Details of these types of information will be provided following acceptance by NASPO of an application for certification.

Theft includes data obtained by gaining unauthorized access to electronic files and transmissions, copying of and physical removal of documents as well as unauthorized verbal communication. Preventing unauthorized access to electronic information that contain data of value to criminal elements requires the partitioning and isolation of data files, implementation of strict access control and effective barriers to unauthorized access. These computer related security requirements and criteria for their implementation are defined in more detail below.

### 5.2.1 IT Security

NASPO auditors will expect to find a set of IT best-practices including the standard use of basic protections such as firewalls, strong authentication, anti-virus software, audit trails, and in some cases, intrusion detection systems. These practices normally result from the existence of a comprehensive and well maintained IT security policy. Practices that NASPO auditors will expect to find include :-

Network Security practices that protect secure data files from both internal and external unauthorized access. Internal file access control will normally involve the use of strong passwords and for very high security applications some form of dual access control that involves authentication of two authorized persons. External or remote access control also requires strong one or two person authentication and barriers such as firewalls to protect against intrusion via the internet and/or wireless based networks. Other precautions include avoiding the use of vendor supplied access defaults and minimizing the opportunity of allowing access by discontinuation of unnecessary services that bring unauthorized persons into close contact with secure files. Details of the specific practices and protective measures that NASPO auditors will expect to find are listed in Table 6.2.1

Identification & Protection of Data that is sensitive and security critical must be carried out. The organization seeking NASPO certification must establish a clear understanding and definition of all computer based data that is (and is not) to be protected by the IT security measures. Having done that, the organization must ensure that such data is securely transmitted or transferred over public networks. As well, if such data has been stored, either temporarily or permanently, the storage media must be purged (wiped clean or destroyed) prior to disposal of the media.

Maintenance of System Security to keep up to date with anti-virus software and patches that are made available from time to time to strengthen barriers to intrusion. The organization must maintain its IT system security to foster a general awareness among system users of defense mechanisms and signs to look for that signal intrusion and data corruption. Vulnerability to intrusion from internet linked systems must be tested from time to time to determine if weaknesses exist and need to be overcome.

Implementation of Access Control to create barriers to unauthorized access mentioned above under Network Security and physical barriers that prevent access to data centers by unauthorized persons. Precautions must also be taken to prevent password fraud at times of resetting and replacement due to loss.

Regular Monitoring and Testing of Networks that enable the organization, at all times, to identify and trace all persons having access to critical data. In operations that handle highly personal and/or sensitive data, NASPO auditors will expect to find that the organization is able to test for and detect unauthorized intrusion using an intrusion detection system (IDS) as detailed below in Section 5.2.1.1. Computer network intrusions that are detected represent a breach of security and must be handled in accordance with the requirements of Section 5.8 and 6.8.

#### 5.2.1.1 Enhanced IT Security Implementation Criteria

Enhancement to IT security, including Intrusion Detection (see Section 6.2.1, NASPO 2-49) and either Dual Secure Data File Access Control (NASPO 2-47) or Biometric Access Control (NASPO 2-48) is mandatory whenever an organization is a custodian of sensitive, computerized personally identifiable information - PII. These enhanced requirements are particularly applicable to operations that involve the use of this data for personalization of any item that may be used as proof of identity or that can in any way be considered to be terrorist enabling.

### 5.2.2 Freedom of Information Laws

Using these laws, copies of bid packages can often be obtained from government organizations. To avoid public disclosure of information of strategic value to unlawful individuals or organizations, NASPO requires organizations to check the applicability of these laws and control disclosure of such information accordingly.

### 5.2.3 Non Disclosure Agreements

Auditors will expect to find widespread use of legal Non-Disclosure Agreements and strict adherence to procedures to prevent disclosure of information judged to be of strategic value (see section 6.9.1 Ref No. 9-2) to unlawful individuals or organizations.

### 5.2.4 The Security Culture

Auditors will expect to see the presence of a security culture that leads both management and employees to respect and honor the need for secrecy, to always be on guard and resist acts of attempted bribery, corruption and infiltration.

### 5.2.5 Reporting of Suspicious Activity

Auditors will expect to find systems in place for the reporting of anything suspicious as well as systems for controlling access to all forms of infiltration.

## 5.3 Security Material Risks

Security materials generally include all materials, tools and devices used in a process that converts the product from a non security to a security product.

Generally, the goal of material control is to accurately account, predict the need for supplies and ensure that the right material is in the right place at the right time. In security products processing this goal is modified by the requirement to minimize, at all times and stages of processing, open access to all special raw materials, special removable tools special computer programs, work in progress and finished product having security value.

NASPO auditors must be satisfied that the opportunity for internal theft of the finished security end item, critical security components and waste having security value has been minimized. As well, NASPO auditors will expect to find a system in use that is able to account to an expected level of accuracy (see 5.1.2 above) for all material in shipping, receiving, secure storage and work in progress.

### 5.3.1 Waste Disposal Risks

In order to prevent fraudulent use being made of waste product and documentation, NASPO requires that all waste be routinely destroyed as part of normal production operations. Whatever method of destruction is used it must not be possible to reconstruct the security product or documentation and fraudulently re-use it. For very high security products, NASPO requires audio/video recording of all destruction operations.

## 5.4 Supply Chain Risks

A supply chain includes all custodial and logistical functions that are performed with the product or service.

The purpose of managing supply chain risks is to ensure that the degree of security assurance required by the product or service is applied uniformly across the whole chain and that no lack of assurance exists in the chain that could endanger the security value of the security end item. The NASPO auditor must be satisfied that the security end item, critical security components or information used to make that end item cannot be subverted or compromised at any point along the chain.

### 5.4.1 Security Material and Security Component Suppliers

Where a security material such as security substrate or a security component such as an optical security device contribute significantly to the ultimate security value of an integrated security end product, the auditor must be convinced that the supplier and all custodial organizations (if any) are assuring the security of those component items at all times up to the time of their delivery to the integrator. For the highest security classes, the auditor must be satisfied that each custodian in the upstream supply chain is actually managing security risks to a degree that is in proportion to the security value of the item delivered. This requirement implies the need for buyers to require suppliers of security components to be certified by NASPO to a class level that is satisfactory and sufficient to assure security of their end items.

### 5.4.2 Sub-Contracting

Sub-contracted work or processing should be avoided wherever possible to take advantage of the benefits to risk management that vertical integration offers. In the event that work on part or the entire security product or service is contracted out, the auditor must be satisfied that the sub-contractor uses the same or an equivalent degree of security risk management as the certified organization. This requirement also implies the need for buyers to require sub contractors to be certified by NASPO to a class level that is satisfactory and sufficient to assure security of their end items.

### 5.4.3 Transportation

Transportation is vulnerable to incidental loss caused by failure of track and trace systems, damage and armed or unarmed theft of security items in transitSpecialized security carriers exist to reduce these risks. For critical, high security products, NASPO auditors will expect to see the use of these specialized carriers. When products are sold where shipping is the responsibility of the end user, organizations must show due diligence in informing the end user of the risks involved in the use of unsecured transportation.

### 5.4.4 Transmitted Documentation

Transmitted documents are vulnerable to innocent disclosure caused by incorrect addressing, fraudulent transmission by an insider, interception and theft. This is particularly true of electronically mailed documents, and some customs and shipping documentation. These types of risk must be substantially reduced by special systems or procedures for all very high security products or services.

### 5.4.5 Custodial Operations

Third party custody of physical security items or information occurs as a normal part of import, export and shipment and whenever shipments are being transferred from one mode of transport to another (e.g. from surface to air). In the case of high security products or components, arrangements must be made by organizations to use secure storage facilities having controlled and recorded access. Those items in custody shall be protected by tamper evident devices.

### 5.4.6 Border Operations

The combination of custodial operations and customs inspection can create risks where anonymous persons might acquire information of strategic value to unlawful individuals or organizations or even gain access to the actual security technology products and components. To reduce these risks, formal arrangements and agreements must be made either directly or via security carriers and brokers for the security products and components to cross the borders and pass through customs free from exposure to these risks.

### 5.4.7 Customs Inspection

Customs officers will normally have been carefully selected and trained, and hence are not expected to pose security threats. Surrounding them, however, are broker personnel and administrative assistants against whom precautions must be taken by making the formal arrangements and agreements outlined in 5.4.6.

### 5.4.8 Letter of Credit Inspectors

Letter of Credit Inspectors are normally appointed by the banks of international customers to verify receipt of correct quantities and qualities. These individuals are normally not security conscious and can potentially pose a security risk. In the event that organizations are faced with these risks, formal arrangements and agreements must be made with the bank of the international customer to assure security.

### 5.4.9 Customer Receiving Operations

Loss of security integrity can occur in customer receiving operations if the area is physically insecure or the personnel are questionable. The risk of theft, falsification of documents and unwanted insider information disclosure exist. For Class I and Class II certification, security products and components suppliers must perform due diligence and assure security in this area.

### 5.4.10 Test and Promotional Samples

Test and promotional samples that closely match characteristics of actual security end items are a potential source of valuable strategic information to any party intent on defeating the security features. Samples might also be fraudulently used in place of authentic security products. For this reason, test samples, especially in transit, must be treated with the same degree of security assurance as the authentic security end items the samples represent.

### 5.4.11 Proof Samples

Proof samples are normally near perfect exemplars of security end items and a perfect source of valuable strategic information for unlawful individuals and organizations. Parties in possession of proof samples could use them to make duplicates for fraudulent purposes. For this reason proof samples must be treated with a degree of security assurance as high as the resulting security end item.

### 5.4.12 Chain of Custody Policy for Distributors & Re-Marketers for the Sale of Security End Items

Where SEI's are supplied to end users through distributor & re-marketing (D&RM) organizations, where the identity of the end user is unknown to the supplier, a Chain of Custody Policy shall be in practice. In addition, the Customer Related Risk Management Requirements specified in Sections 5.1 and 6.1 shall apply.

The Chain of Custody policy shall address as a minimum :-

- USE OF SECURITY TECHNOLOGIES AND/OR PRODUCTS; D&RM's shall be bound by legal agreement to obtain prior approval from the supplier for the sale of all security technologies, materials, end items or services to end users. In addition, D&RM's shall be legally bound, with all due diligence, to avoid all sales that may involve fraudulent, phony or illegal end uses.

- CERTIFICATION OF END-USER; The end-user must qualify as a legitimate user in accordance with Sections 5.1 & 6.1 of this Standard.

- DESTINATION OF SHIPMENTS; All SEI's must be tracked and shipped only to the qualified end-user. Suppliers must not ship SEI's to D&RM's without prior approval from qualified end users.

- RETENTION OF INFORMATION; As an aid to enforcement of its security procedures, D&RM's must agree to maintain records for three years that track the distribution and use of SEI's. The D&RM's must be made aware that they may be required to provide copies of these records to the SEI supplier for a period of three (3) years.

- RE-MARKETING; All SEI's are expressly prohibited from being sold to any unknown end user.

- APPLICABLE LAW; The Chain of Custody Agreement shall identify the legal jurisdiction under which the parties have agreed to be legally bound.

### 5.4.13 Other Supply Chain or Logistical Risk Areas

It is unlikely that the supply chain risks covered so far in this section are exhaustive and perfectly applicable to all organizations. For this reason, NASPO auditors will, at the outset of their audits, carry out a review with the organization regarding the applicability of these risks and the need to tailor the criteria that follow to cover risks specific to the organization's products or services. For example, organizations who are importing critical security components from countries outside Canada and the USA may face additional risks requiring special control measures.

## 5.5 Physical Intrusion Risks

In order to avoid the consequences of physical intrusion, NASPO requires the use of access control systems by all of its certified organizations. Organizations involved in the making of very high security products, especially those that may be terrorist enabling, carry high economic value, or life consequences, must implement systems that are capable of establishing a persons identity beyond a reasonable doubt. In such cases, NASPO auditors will expect to see a very high level of physical intrusion detection and resistance in all buildings, facilities and information rich offices. In cases where violent (armed) robberies or hostage situations are possible, armed guarding, dogs and perimeter fencing may also be required.

## 5.6 Personnel Risks

NASPO auditors must be assured that no employees or personnel of the company, involved in any way with physical security items or information, have any history of fraudulent wrong doing. In the event that hard evidence has been found by or comes to the attention of the organization from past employment, credit rating, or other records, NASPO certification requires corrective action be taken to isolate, neutralize or terminate the persons involved.

In general, NASPO auditors will expect to find personnel policies and procedures in place that will substantially reduce the risk of fraud from company personnel. Included in those procedures should be polices that address employment screening, background checks, and termination policies.

The auditors will also expect to see that the company is proactive in building and maintaining a security culture, diligent in providing security procedures training and in maintaining a high level of preparedness in all personnel.

## 5.7 Disaster Recovery Risks

Disasters can be man-made or natural. Arson and tornado's are examples. Whatever the cause, the result will usually involve entrance of emergency personnel into the building and a breakdown of some, or all security systems and infrastructure that normally prevent fraud. In order to assure security, in the face of such disasters, NASPO auditors will expect to see plans in place and preparedness aimed at maintaining security in spite of such a disaster. These documents are typically found in the Company Security Policy Manual or the Disaster Recovery Plan. In the event that the organization is under a contractual obligation to be "fail operational", regardless of the nature of the catastrophe, NASPO auditors will expect to find that the level of security assurance applied to normal operations is also applied in the backup operation that enables the organization to continue to securely produce and deliver.

## 5.8 Security Failure Risks

To prepare for the possibility of security assurance failures or breaches, NASPO auditors will generally expect to find a system of control and accountability within the organization. The system should demonstrate the ability to track materials and personnel as the products are being produced. The system should be able to identify those areas within the process that have failed, and provide procedures to remedy those failures.

In the case of high security product producers it is important to be able to isolate the cause of the breach by retracing events that lead up to it. To this end, NASPO auditors will expect to find systems in operation that provide:-

- a time history record of the location of all personnel and visitors within the premises and their activities at the time of the breach.
- the origin and batch identity of all materials used to make the SEI's
- a time history record of all material handling operations.

- video tape or digitized video records of key security areas.
- detection of missing security materials or security sensitive Information.

Resources, in the form of security management personnel, must also be available to log, analyze and document each breach and plan and implement corrective action to prevent the same failures from occurring again.

## 5.9 Security Management Risks

The functions of security management must be successfully performed by the organization to comply with this version of the ANSI/NASPO security assurance standard. The functions must include a comprehensive and ongoing identification and analysis of security threats and vulnerabilities and an assessment of the need to eliminate or reduce significant risks implied by the findings that are not already covered by any of the mandatory risk reduction requirements specified in section 6 below. Overall, security risk management must aim to detect and respond to new and emerging threats and vulnerabilities and comply on an ongoing and day to day basis with the security assurance requirements of this standard.

## 5.10 Other Risks

It is unlikely that the security risks covered so far in this section are exhaustive and perfectly applicable to all organizations. For this reason, NASPO auditors will, at the outset of their audits, carry out a review with the organization regarding the applicability of these risks, and the need to tailor the criteria that follow to cover risks specific to the organization seeking certification. For example, organizations who are responsible for personalizing documents, whether cards or paper documents, must secure the personal data in order to comply with privacy laws that require personal information security.

(back to Table of Contents )

**The balance of this page is intentionally left blank.**

# 6.0 Risk Management Objectives & Certification Criteria

## 6.1 Customer Related Risk Management Objectives

**Class I** To enter into supply contracts only with customers who are, without doubt, bona fide and who use and maintain verifiable controls and procedures to prevent unauthorized purchase, distribution or illegal use of a security product.

**Class II** To enter into supply contracts only with customers who are, beyond a reasonable doubt, bona fide and who use and maintain verifiable controls and procedures to prevent unauthorized purchase, distribution or illegal use of a security product.

**Class III** To be vigilant in the identification of potential customers who may be fraudulent and be willing to refuse to supply any security product samples or enter into supply contracts with any entity until firm evidence indicates that they are bona fide.

### 6.1.1 Customer Related Risk Management Certification Criteria

| **Ref. No.** | **Certification Criteria**<br>**M = Mandatory ; E = Enhancement (see Section 4.0) definitions Appendix A1** | **Class I** | **Class II** | **Class III** |
|---|---|---|---|---|
| 1-1 | State/Federal confirmation of business | **M** | **M** | **M** |
| 1-2 | Written financial references | **M** | **M** | **M** |
| 1-3 | Written corporate references | **M** | **M** | **M** |
| 1-4 | Contract/document specifying product use | **M** | **E** | **E** |
| 1-5 | Evidence of Authorization from end user | **M** | **E** | **E** |
| 1-6 | Written detail of Customer Ordering processes | **M** | **M** | **M** |
| 1-7 | Written designation of authorized personnel | **M** | **M** | **E** |
| 1-8 | Verifiable signatures/passwords for authorized personnel | **M** | **E** | **E** |
| 1-9 | Secured storage for all requisition/ authorization, whether hard copy or electronic, documents | **M** | **M** | **M** |
| 1-10 | Written report by third party investigative agency re purchasing entity. | **E** | **E** | **E** |
| 1-11 | Written confirmation by regulating agency | **E** | **E** | **E** |

## 6.2 Information Risk Management Objectives

**Class I** To prevent **all** unwanted or unintended disclosure of information of potential strategic value to terrorists, syndicates, cartels or other unlawful third party individuals and organizations with serious intent to acquire, circumvent, mimic or subvert security technologies or services and to fully mitigate any effects, impact, and consequences caused by unwanted or unintended disclosure should such an event occur.

**Class II** To prevent unwanted or unintended disclosure of information of potential strategic value to terrorists, syndicates, cartels or other unlawful third party individuals and organizations with serious intent to acquire, circumvent, mimic or subvert security technologies or services and to mitigate the effects, impact, and consequences caused by unwanted or unintended disclosure should such an event occur.

**Class III** To be aware of the need and act to avoid disclosure of selected information of potential strategic value to third party individuals and organizations with serious intent to acquire, circumvent, mimic or subvert security technologies or services and to act quickly to mitigate the effects and consequences caused by unwanted or unintended disclosure should such an event occur.

### 6.2.1 Information Risk Management Certification Criteria

| Ref No. | **Certification Criteria**<br>**M = Mandatory ; E = Enhancement (see Section 4.0)** | Class I | Class II | Class III |
|---|---|---|---|---|
| General Information Risk Reduction Criteria - definitions Appendix A2 | | | | |
| 2-1 | "Need to Know " Policy | M | M | M |
| 2-2 | Information Disclosure Evaluation | M | M | M |
| 2-3 | Voice/Photo/Video Recording Device Control | M | M | E |
| 2-4 | Strict use of Disclosure Agreements | M | M | M |
| 2-5 | Strict Use of Fax & eMail Confidentiality Notes | M | M | E |
| 2-6 | Security Evaluation of Sales Literature | M | M | M |
| 2-6 | Security Evaluation of Web Site Content | M | M | M |
| 2-6 | Security Evaluation of News Releases | M | M | M |
| 2-6 | Security Evaluation of Security Commission Reports | M | M | E |
| 2-6 | Security Evaluation of Trade Show Materials | M | M | M |
| 2-6 | Security Evaluation of Conference Presentations | M | M | E |
| 2-6 | Security Evaluation of Annual Reports | M | M | E |
| 2-6 | Censoring of all Public Disclosure | M | E | E |
| 2-7 | Secrecy Training | M | M | E |
| 2-8 | Security Awareness Program | M | M | M |
| 2-9 | Visual Intrusion Barriers | E | E | E |
| 2-10 | Communication Monitoring | E | E | E |

| | | | | |
|---|---|---|---|---|
| 2-11 | Centralized Call Receiving | E | E | E |
| 2-12 | Witnessed Meeting Procedure | E | E | E |
| 2-13 | Complete Destruction of Documentation | M | M | M |
| 2-14 | Wire Tap Protection | E | E | E |
| 2-15 | Use of False Data Trails | E | E | E |
| 2-16 | Remote Listening System Evaluation | E | E | E |
| IT (Computer) Risk Reduction Criteria – definitions Appendix A2 | | | | |
| 2-17 | Formal IT Security Risk Manager | M | M | M |
| 2-18 | A Taking Work Home Policy | M | E | E |
| 2-19 | Secure File Transfer Track & Trace | M | E | E |
| 2-20 | Computer Access Control using Passwords or other Strong Authentication. | M | M | E |
| 2-21 | Secure File Access Control | M | M | E |
| 2-22 | Secure External Data Transfer or Transmission | M | M | E |
| 2-23 | Destruction of Media | M | M | M |
| 2-24 | Secure Wireless Transmission | M | M | M |
| 2-25 | Separate Web and File Servers | M | M | M |
| 2-26 | Laptop File Transfer Policy & Procedure | M | E | E |
| 2-27 | Recordable Media Removal Policy | M | E | E |
| 2-28 | Firewall on External Connections | M | M | M |
| 2-29 | Vulnerability Scanning | M | M | M |
| 2-30 | Password reset procedures | M | M | M |
| 2-31 | Computer Virus Protection | M | M | M |
| 2-32 | Security Patching | M | M | M |
| 2-33 | Account lockouts | M | M | M |
| 2-34 | Physical Access Control of IT Systems | M | M | M |
| 2-35 | Track and monitor network access | M | M | M |
| 2-36 | Log and Review Critical Events | M | M | M |
| 2-37 | Maintain System Logs | M | M | M |
| 2-38 | Test Security Systems | M | M | M |
| 2-39 | Incident Response Plan | M | M | M |
| 2-40 | Maintain a current network diagram | E | E | E |
| 2-41 | Change control process for IT systems | E | E | E |
| 2-42 | Remove Vendor Defaults | E | E | E |
| 2-43 | Disable Unnecessary Services | E | E | E |
| 2-44A | Strong Authentication for Remote Access. | M | M | M |
| 2-44B | Strong Encryption for Remote Access. | M | M | E |
| 2-45 | Protect Backup Media | M | M | E |
| 2-46 | Sanitize Media Before Disposal | E | E | E |
| 2-47 | Dual access control for secure data files that contain personal identity information (PII). | E/M | E/M | E/M |
| 2-48 | Secure Data File Access Control using Biometric Measurement | E | E | E |

| | | | | |
|---|---|---|---|---|
| 2-49 | Secure Data File Intrusion Detection System | E/M | E | E |

Note ; E/M signifies that these requirements may be Mandatory – refer to 5.2.1.1

## 6.3 Material Risk Management Objectives

**Class I** To prevent all theft of all security materials, and at all times be able to detect if materials are missing.

**Class II** To deter and prevent theft of critical security materials, and at all times be able to detect if critical security materials are missing.

**Class III** To minimize opportunities for theft to occur, and at all times be able to detect if materials are missing.

### 6.3.1 Material Risk Management Certification Criteria

| Ref. No. | **Certification Criteria**<br>**M = Mandatory ; E = Enhancement (see Section 4.0)**<br>**definitions Appendix A3** | **Class I** | **Class II** | **Class III** |
|---|---|---|---|---|
| 3-1 | Deleted - see NASPO 5-15. | | | |
| 3-2 | Internal secured storage | M | M | M |
| 3-3 | Restricted access areas | M | M | M |
| 3-4 | Incoming inspection | M | M | M |
| 3-5 | Secured disposal of waste | M | M | M |
| 3-6 | Inventory control | M | M | M |
| 3-7 | Material discrepancies report | M | M | M |
| 3-8 | Vault storage of secure materials | M | E | E |
| 3-9 | Vault storage of finished goods | M | E | E |
| 3-10 | Precise accounting at unit level | M | M | M |
| 3-11 | Written cycle counting policy & procedure | E | E | E |
| 3-12 | Multiple signatures and witnesses | E | E | E |
| 3-13 | Accountability of In process materials | E | E | E |

**The balance of this page is intentionally left blank.**

## 6.4 Supply Chain Risk Management Objectives

**Class I** To prevent the possibility, at any point in the supply chain or production process, of any fraudulent acts from subverting or in any way compromising the security value of all of the Organizations security products and related services. To do this, the Certified Organization must demonstrate the existence of, or capability to establish, the documented controls and procedures that trace all security materials and technology from all sources to all points of issue.

**Class II** To deter and prevent the possibility, at any point in the supply chain or production process, of any fraudulent acts from subverting or in any way compromising the security value of the Organization's critical security products and related services.

**Class III** Be aware of and demonstrate an understanding and recognition of the need to control supply chain risks and have the ability to act accordingly.

### 6.4.1 Supply Chain Risk Management Certification Criteria

| Ref. No. | **Certification Criteria**<br>**M = Mandatory ; E = Enhancement (see Section 4.0) definitions Appendix A4** | Class I | Class II | Class III |
|---|---|---|---|---|
| General Supply Chain Controls: | | | | |
| 4-1 | State/Federal confirmation of business | M | M | M |
| 4-2 | Written financial references | M | M | M |
| 4-3 | Written corporate references | M | M | M |
| 4-4 | Written report by third party investigative agency re supplier of critical materials entity. | M | M | E |
| 4-5 | Deleted - see NASPO 1-5 | | | |
| Upstream Supplier Controls: | | | | |
| 4-6 | Written designation of authorized supplier personnel | M | M | E |
| 4-7 | Written document that demonstrates recognition of the need to control supply chain risks | M | M | M |
| 4-8 | Signatures of understanding of the need to control supply chain risks from all personnel involved with security sensitive materials, devices, technology, or information who interact with the supply chain. | M | M | M |
| 4-9 | Documented track & trace for all shipments, including transportation, weight, quantity, trans-shipments, secondary shipments, and | M | E | E |

| | | | | |
|---|---|---|---|---|
| | final destination. | | | |
| 4-10 | Periodic third-party audits | M | M | M |
| 4-11 | Documented inspection of all incoming security materials | M | M | M |
| In-House Supply Chain Controls: | | | | |
| 4-12 | Documented confirmation of security products end use | M | E | E |
| 4-13 | Delete - see NASPO 8-2 | | | |
| 4-14 | Reciprocal Non Disclosure Agreements with Supply Chain Players | M | M | E |
| 4-15 | Chain of Custody Policy with Distributors and re-Marketers | M | M | E |
| 4-16 | Written detail of Purchase ordering procedures | M | M | M |
| 4-17 | Secured storage for all Purchase requisition/ authorization, whether hard copy or electronic, documents | M | M | M |
| 4-18 | In-house audit procedures | E | E | E |
| Downstream Customer Controls: | | | | |
| 4-19 | Contract/document specifying product use rules | M | E | E |
| 4-20 | Written report by third party investigative agency re firms to which security products will be supplied. | E | E | E |
| 4-21 | Written confirmation by regulating agency re ; authenticity of end-user and/or firms to which security will be supplied. | E | E | E |
| 4-22 | Verifiable signatures/passwords for authorized personnel | E | E | E |
| 4-23 | Second person review of all orders/shipments | E | E | E |
| 4-24 | Inspection/audit of facility to which security products are shipped to insure security compliance | E | E | E |
| 4-25 | Transportation assurance when security sensitive goods are sold FOB the supplier's shipping dock. | M | M | E |
| 4-26 | Transportation assurance procedure | M | M | E |

**The balance of this page is intentionally left blank.**

## 6.5 Physical Intrusion Risk Management Objectives

**Class I** To create layers of physical intrusion resistance and alarms into secure physical and sensitive information areas of the facility that will ensure the arrival of local law enforcement or armed security personnel before intruders have time to gain access to and leave with sensitive physical and/or information items.

**Class II** To create layers of physical intrusion resistance and alarms that will delay intrusion into sensitive physical and/or information areas sufficient to provide local law enforcement or security personnel with a realistic time frame to arrive in time to apprehend intruders.

**Class III** To create layers of physical intrusion resistance and alarms that will delay intrusion into sensitive physical and/or information areas sufficient to provide local law enforcement or security personnel with a realistic time frame to arrive in time to apprehend intruders.

### 6.5.1 Physical Intrusion Risk Management Certification Criteria

| Ref. No. | **Certification Criteria**<br>M = Mandatory ; E = Enhancement (see Section 4.0) definitions Appendix A5 | Class I | Class II | Class III |
|---|---|---|---|---|
| Perimeter Security : | | | | |
| 5-1 | Exterior Surveillance | M | E | E |
| 5-2 | Controlled Access Exterior Doors | M | M | E |
| 5-3 | Alarmed Entrances | M | M | M |
| 5-4 | Alarmed Emergency Exits | M | M | M |
| 5-5 | Exterior Lighting | M | M | M |
| 5-6 | Secure Exterior Walls | M | M | E |
| 5-7 | Monitored Exterior Windows | M | M | M |
| 5-8 | Controlled Roof Access | M | M | M |
| 5-9 | Physical Perimeter Barriers | E | E | E |
| 5-10 | Guard Monitored Perimeter | E | E | E |
| Interior Security: | | | | |
| 5-11 | Main Entrance Controlled Access | M | E | E |
| 5-12 | Visitor Access Control & Recording | M | M | M |
| 5-13 | Internal Secure Areas | M | M | M |
| 5-14 | Vault Area | M | E | E |
| 5-15 | Interior Surveillance | M | M | E |
| 5-16 | Waste Destruction Area | M | M | E |
| 5-17 | Motion Detection | M | M | E |
| 5-18 | Fire and Smoke Detection | M | M | M |
| 5-19 | Internal Emergency Alarm System | M | E | E |
| 5-20 | Restricted Access Areas | M | M | M |

| | | | | |
|---|---|---|---|---|
| 5-21 | Controlled Shipping and Receiving | M | M | E |
| 5-22 | Guard Controlled Access | E | E | E |
| 5-23 | Security Control Room | M | M | E |
| 5-24 | Dual Control Access | E | E | E |
| 5-25 | Dress Codes for Restricted Areas | E | E | E |
| 5-26 | External Emergency Alarm System | E | E | E |
| Facility Security Procedures: | | | | |
| 5-27 | Key Controls | M | M | M |
| 5-28 | Vault Combination/Key Controls | M | E | E |
| 5-29 | Remote Monitor Media Control | M | M | E |
| 5-30 | Policies, Procedures and Preparedness for the Management of Physical Intrusion | M | M | M |
| 5-31 | Deleted - see NASPO 5-30 | | | |
| 5-32 | Deleted - see NASPO 5-30 | | | |
| 5-33 | Security System Backup Power Supply | M | M | E |
| 5-34 | Access Control Monitoring | E | E | E |
| 5-35 | Deleted - see NASPO 5-30 | | | |
| 5-36 | Prevention of Unauthorized Multi Person Access (commonly known as “piggy backing”) to Secure or Restricted Areas using the Identity and Access Permission of a Single Person. | M | M | E |

**The balance of this page is intentionally left blank.**

## 6.6 Personnel Risk Management Objectives

**Class I** To eliminate and prevent all personnel related fraud. To this end, a Class I Certified Organization shall be operating under a personnel policy that results in the highest level of security practices that cover initial hiring, operational personnel security practices, security awareness and education, and employee termination.

**Class II** To reduce, to a reasonable level of risk, all personnel fraud. To this end, a Class II Certified Organization must incorporate a moderate level of security practices that cover initial hiring, operational personnel security practices, security awareness and education, and employee termination.

**Class III** Be able to detect and act on behaviors or suspicious actions of personnel within the Organization that do not comply with the basic integrity required within the industry. To this end, a Class III Certified Organization must be operating under a personnel policy that includes security practices related to initial hiring, operational personnel security practices, security awareness and education, and employee termination.

### 6.6.1 Personnel Risk Management Certification Criteria

| Ref. No. | **Certification Criteria**<br>**M** = Mandatory ; **E** = Enhancement (see Section 4.0) | Class I | Class II | Class III |
|---|---|---|---|---|
| **Background Checks – definitions Appendix A6** | | | | |
| 6-1 | Employer References | M | M | M |
| 6-2 | Credit | M | M | E |
| 6-3 | Criminal | M | M | M |
| 6-4 | Drug Screen | M | M | M |
| 6-5 | Social Security Number Verification | M | M | M |
| 6-6 | Annual Credit Check | E | E | E |
| 6-7 | Motor Vehicle Violations | E | E | E |
| 6-8 | Formal Education | E | E | E |
| 6-9 | Fingerprint Screen | E | E | E |
| **Personnel Policies and Procedures:** | | | | |
| 6-10 | Fingerprinting | M | E | E |
| 6-11 | Photographs | M | M | M |
| 6-12 | Employee Security Policy | M | M | M |
| 6-13 | Company Security Policy | M | M | M |
| 6-14 | Annual Employee Security Training | M | M | E |
| 6-15 | Security Management Responsibility | M | M | M |
| 6-16 | Security Guard Policies and Procedures | M | E | E |
| 6-17 | Use of Internal Security Awareness Communications | M | M | M |
| 6-18 | Psychological Testing/Screening | E | E | E |

## 6.7 Disaster Recovery Risk Management Objectives

**Class I** To protect against any and all security breakdowns that result from either man made or natural disasters. To this end, a Class I Certified Organization must have in effect a disaster security plan. This plan will reflect a high degree of preparedness in the prevention of any loss of control of secure products or materials. This plan may include the use of force or armed personnel to ensure the integrity of resources.

**Class II** To protect against potential security breakdowns that result from either man made or natural disasters. To this end, a Class II Certified Organization must have in effect a disaster security plan. The plan must provide a level of preparedness that will ensure a minimal loss of security products and materials. This plan shall include the use of designated personnel to ensure the integrity of resources.

**Class III** To recognize the need to protect security products and materials from security breakdowns that might result from either man made or natural disasters. To this end, a Class III Certified Organization must have in effect a disaster security plan that aims to minimize the loss of those products and materials deemed as requiring security assurance.

### 6.7.1 Disaster Recovery Risk Management Certification Criteria

| Ref. No. | **Certification Criteria**<br>**M** = Mandatory ; **E** = Enhancement (see Section 4.0) definitions Appendix A7 | Class I | Class II | Class III |
|---|---|---|---|---|
| 7-1 | Plan for Securing Facilities | M | M | M |
| 7-2 | Data and Information Security Plan | M | M | M |
| 7-3 | Use of Armed Personnel in Event of Disaster | M | M | E |
| 7-4 | Chemical/Biological Incident Plan | M | E | E |
| 7-5 | Terrorist / Armed Intruder Attack Plan | M | E | E |
| 7-6 | Use of Uniformed Personnel in Event of Disaster | M | M | M |

**The balance of this page is intentionally left blank.**

## 6.8 Security Failure Risk Management Objectives

**Class I** The ability to detect, analyze and prevent the re-occurrence of all breaches of security.

**Class II** The ability to detect, analyze and prevent the re-occurrence of breaches of security that result in serious consequences.

**Class III** Awareness of the need to prevent re-occurrence of serious security breaches and some ability to detect, analyze and act to prevent future breaches in a systematic manner.

### 6.8.1 Security Failure Risk Management Certification Criteria

| **Ref. No.** | **Certification Criteria**<br>**M = Mandatory ; E = Enhancement (see Section 4.0) definitions Appendix A8** | **Class I** | **Class II** | **Class III** |
|---|---|---|---|---|
| 8-1 | Security Breach Incident Log | **M** | **M** | **M** |
| 8-2 | A Written Breach Handling Procedure | **M** | **M** | **M** |
| 8-3 | A Designated Breach Manager | **M** | **M** | **M** |
| 8-4 | Failure Modes & Effects Analysis of Selected (Critical Only) Security systems | **M** | **M** | **E** |
| 8-5 | Plans & Preparations for Recovery & Mitigation of Effects | **M** | **M** | **E** |
| 8-6 | Company & Employee Legal Liability Awareness | **M** | **M** | **M** |
| 8-7 | Links with Crime & Intelligence Agencies | **M** | **E** | **E** |
| 8-8 | Historical Breach Experience Reports | **M** | **M** | **M** |
| 8-9 | A Critical Security Area Monitoring System | **M** | **M** | **E** |
| 8-10 | Security Breach Informing System (Ears & Eyes) | **M** | **M** | **M** |
| 8-11 | A Working Relationship with Law Enforcement | **M** | **M** | **M** |
| 8-12 | A Comprehensive Failure Modes & Effects Analysis | **E** | **E** | **E** |
| 8-13 | Links with Interpol | **E** | **E** | **E** |
| 8-14 | Automated Material Track & Trace system | **E** | **E** | **E** |
| 8-15 | A Personnel Track & Trace system | **M** | **E** | **E** |
| 8-16 | A Document Track & Trace system | **E** | **E** | **E** |

## 6.9 Security Risk Management Related Objectives

**Class I**

- Assure Class I security at all times by continuous compliance with Class I requirements.
- Avoid all breaches of security and fully mitigate any that occur.
- Anticipate new forms of threat, identify new vulnerabilities and new risks being taken.
- Formulate and implement new countermeasures to maintain security in the face of new threats and vulnerabilities.
- Be able to demonstrate to existing and potential new customers that the only security risks they are taking, in doing business with the organization, are those that fall outside the risk reduction scope of Class I.
- Develop and fully maintain a Class I security culture
- Develop and maintain a succession plan to assure continuous performance of all Class I security assurance jobs and tasks.
- Participate in professional development programs in order to improve knowledge of security assurance techniques and on-the-job performance.

**Class II**

- Assure Class II security at all times by continuous compliance with Class II requirements.
- Avoid breaches of security having serious consequences and mitigate the effects of any that occur to a degree that avoids customers losing confidence in security assurance of the organization.
- Anticipate new forms of threat, identify new vulnerabilities and new risks being taken.
- Formulate and implement new countermeasures to maintain security in the face of new threats and vulnerabilities.
- Be able to demonstrate to existing and potential new customers that the only security risks they are taking in doing business with the organization are those that fall outside the risk reduction scope of Class II.
- Develop and fully maintain a Class II security culture
- Develop and maintain a succession plan to assure continuous performance of vital security assurance jobs and tasks.
- Occasionally participate in professional development programs in order to improve knowledge of security assurance techniques and on-the-job performance.

**Class III**

- Assure Class III security at all times by continuous compliance with Class III requirements.
- Avoid major breaches of security and fully mitigate any that occur.
- Inquire about new forms of threat, new vulnerabilities and new risks being taken.
- Consider formulating and implementing new countermeasures to maintain security in the face of new threats and vulnerabilities.
- Be able to demonstrate to existing and potential new customers that the only security risks they are taking in doing business with the organization are those that fall outside the risk reduction scope of Class III.
- Develop and fully maintain a Class III security culture

- Develop and maintain a succession plan to assure continuous performance of all Class III security assurance jobs and tasks.
- Consider participating in professional development programs in order to improve knowledge of security assurance techniques and on-the-job performance when higher security demands are experienced by the organization.

## 6.9.1 Security Risk Management Related - Certification Criteria

| Ref. No. | **Certification Criteria**<br>**M = Mandatory ; E = Enhancement (see Section 4.0) definitions Appendix A9** | Class I | Class II | Class III |
|---|---|---|---|---|
| 9-1 | Perform Security Risk Management | M | M | M |
| 9-2 | Identify & Classify all Security Sensitive Physical and Information Items | M | M | M |
| 9-3 | Perform Security Threat Identification & Analysis | M | M | M |
| 9-4 | Perform Security Vulnerability Identification and Analysis | M | M | M |
| 9-5 | Perform Security Risk Identification, Analysis and Assessment | M | M | M |
| 9-6 | Designated Security Manager | M | M | M |
| 9-7 | Designated IT Security Risk Manager | M | M | M |

(back to Table of Contents )

**The balance of this page is intentionally left blank.**

# 7.0 Security Assurance - Verification

All audits carried out by NASPO will aim to verify that organizations have developed a sharp awareness of possible fraudulent actions specific to their security product and/or service portfolio, recognize that they pose a threat to the value of their security products, implement countermeasures aimed at preventing them, put plans in place and be prepared to mitigate their effects in the event that fraudulent acts occur.

Verification of the above will be carried out by NASPO auditors (or commercial certification bodies accredited by NASPO) who will use a combination of:-

- **Documentary Evidence**
- **Experience Reports**
- **Analysis Reports**
- **Interviews**
- **Site Visits**
- **Simulations**
- **Similarity with other Proven Systems**
- **Demonstration**
- **Testing**

to prove that security assurance is being delivered in accordance with the requirements of the Class for which the organization is seeking certification. All NASPO audits will be carried out under a strict Confidentiality Agreement.

## 7.1 Summary of the Audit Process

Audits will be carried out in a sequence of steps as follows.

**Step 1 - Application & Class Confirmation**

The audit will begin with completion of an Audit Application & Self Assessment form. The contents of this form will enable NASPO auditors to confirm appropriateness of the class for which the organization is seeking Certification. Confirmation of appropriateness of class will involve an assessment of vulnerability to “attack” and seriousness of consequences of the product or information falling into the wrong hands. In the event that the certification class is disputed and cannot easily be resolved by the auditor, the matter will be referred to the NASPO Certification Committee for resolution.

The Audit Application Form is expected to require the following data:-

- Definition of the nature and end use of the organization’s security product portfolio.
- Percentage of time that the organization operates as a security products producer.
- Name of the single point contact responsible for Security Assurance.
- A brief description of the infrastructure and systems dedicated to Security Assurance.
- An estimate of capital invested overall in Security Assurance.

- The annual budget allocated exclusively for Security Assurance.
- A brief description of personnel resources dedicated to the performance of Security Assurance.
- A brief description of the supply chain associated with the core security products of the company

### Step 2 - Audit Data Requirements

Having confirmed the certification class in Step 1, organizations must provide NASPO with at least two copies of a pre-audit data package specified by the designated NASPO auditor. The data package, as a minimum, will request documents that address company security policy and procedures. Contained in these documents NASPO auditors will expect to find the awareness, recognition of threats, countermeasures and mitigation plans outlined in the Introduction. In the event that such documentation does not exist, cannot be furnished or is totally inadequate, the audit will be deferred until it becomes available.

### Step 3- Evaluation and Reporting

In this step NASPO auditors will evaluate the degree to which the organization is in control of relevant security risks and delivering security assurance in compliance with the requirements of the certification class sought. In general, the auditor must be granted access to sites involved with the production of security items, or delivery of security services, to evaluate conformance to requirements. In all cases, a report will be delivered to the organization to convey the findings with recommendations either for improvement, if required, or corrective action in the case of a clear failure to comply.

### Step 4 - Rectification and/or Certification

In the event that an organization fails to comply, auditors will work with the organization to create a plan for rectification and may return to the organization to verify that rectification has taken place. At this point, a certificate will be issued by the NASPO Executive Committee or commercial certification body. Certification applicants who are clearly compliant and in no need of either improvement or corrective action will receive a certificate upon completion of the mandatory auditors report.

### Step 5 – Surveillance Audits

In order to verify ongoing compliance with the ANSI/NASPO standard, surveillance audits will be carried out 12 months and 24 months following the award of a security assurance certificate. These surveillance audits will verify that all security assurance jobs and tasks are continuing to be performed and new risks (resulting from either new threats or vulnerabilities or changes in product or service portfolio) are known and being properly managed.

### Step 6 – Re- Certification

Organizations wishing to maintain their security assurance certification beyond three years must undergo a full certification audit after 36 months from the initial award date.

(back to Table of Contents )

# APPENDIX A - Criteria Definitions

The following definitions refer to the Certification Criteria items tabulated in Section 6 above. The definitions below clarify the meaning of each certification criteria.

## A1 - Customer Related Criteria Definitions

**1-1 State/Federal confirmation of business**; This is confirmation provided by a state, province or federal business registration authority of the registration or ID number of the potential customer. (back to 6.1.1)

**1-2 Written financial references**; This is a recognized independent financial report, such as a bank reference, a Dunn & Bradstreet (or equivalent) report or other disclosure from a recognized financial institution, that clearly shows that the potential customer is in good financial standing. (back to 6.1.1)

**1-3 Written corporate references**; A written corporate reference is a letter or document issued by an independent third party corporation in favor of the potential customer. It is expected that this reference will state that the independent corporation has (over the previous 3 years) or is doing business with the potential customer to the satisfaction of the third party corporation. In the case of companies less than 3 years old, past reputation or personal references of senior personnel for observing security protocols will be considered in lieu of corporate references. (back to 6.1.1)

**1-4 Contract/document specifying product use**; This is a copy of a binding supply contract or purchase order which clearly specifies the end use of the potential customer's product. If clear specification of end use is not contained in any of these documents, referenced RFP or RFQ which clearly define the end use should be sought as an alternative. In cases where customers are unwilling to disclose the end use, some form of assurance issued to the supplier by the customer that indicates that it will not be misused and will be protected to avoid loss of value to other users, will be considered in lieu of evidence from supply contracts, purchase orders, RFP's or RFQ's. (back to 6.1.1)

**1-5 Evidence of Authorization from End User;** The end user will normally be an issuing authority, governmental agency or brand owner. Written confirmation must clearly show that the end user is aware of and has authorized the potential customer to procure the security feature from the accredited company on its behalf. (back to 6.1.1)

**1-6 Written detail of Customer Ordering processes**; These procedures apply to orders placed by customers of security materials or items. It is important to know that these orders have been officially sanctioned both internally and externally. The detail is intended to show what information flows back and forth in the process of completing the placing and acceptance of an order for security end items. (back to 6.1.1)

**1-7 Written designation of authorized personnel**; In this case the writer must be either the corporate secretary or a senior executive of the potential customer. The written designation must identify those persons who have been authorized to decide and act on behalf of the potential customer on all matters related to the procurement of the company's security product(s). (back to 6.1.1)

**1-8 Verifiable signatures/passwords for authorized personnel**; Verifiable signatures are exemplars of the hand written signatures of all personnel who the potential customer has notified in writing will decide and act on it's behalf in all matters related to the procurement of the organization's security product(s). The passwords used shall enable the organization to know the identity of the person who has sought access to the password controlled system. (back to 6.1.1)

**1-9 Secured storage for all requisition/authorization, whether hard copy or electronic, documents**; Secured storage means that access to the store (whether a vault, safe, cabinet or computer file) is restricted to formally authorized personnel who have been security cleared as a result of the background checks required under section 6. (back to 6.1.1)

**1-10 Written report by third party investigative agency re purchasing entity**; This is a report commissioned and paid for by the organization seeking Certification. The contents of the report are expected to indicate that the potential customer is bona fide, and free from past and present behavior that are indicative of either fraudulent activity or security irresponsibility. (back to 6.1.1)

**1-11 Written confirmation by regulating agency**; In this case, the regulating agency has been cited by the potential customer as the end user of the security product to be supplied by the potential customer. Preferably in written form, this is confirmation by the regulating agency (usually an issuing authority or governmental agency) that the supply contract claims of the potential customer are true. (back to 6.1.1)

## A2 - Information Criteria Definitions

**2-1 "Need to Know Only" Policy**; A "need to know" test will always be performed whenever information that is judged to be of strategic value is disclosed to anyone. All personnel including all executives shall be given information of strategic value only on a need to know basis. It is expected that this procedure will protect unwanted disclosure of this type of information without disabling the free flow of information that is required in a solutions oriented security products company. (back to 6.2.1)

**2-2 Information Disclosure Evaluation**; This is the act of evaluating the security risk of all visitors and then controlling their access to both physical areas of a building and information. Such control will normally involve execution of a Non Disclosure Agreement. (back to 6.2.1)

**2-3 Voice/Photo/Video Recording Device Control**; Means controlling both internal and visitor use of all devices that are capable to recording voice, photographic and live action video data in all secure areas of a building. (back to 6.2.1)

**2-4 Strict use of Disclosure Agreements**; There are no exceptions. All personnel must enter into a legally binding Non-Disclosure Agreement prior to the exchange of any information of potential strategic value or confidential nature. (back to 6.2.1)

**2-5 Strict use of Fax & eMail Confidentiality Notes;** There are no exceptions. All faxes and emails must include as a header, footnote or included in the message, wording that indicates to the reader that the information received is considered to be confidential by the sender, should be treated as such and if received in error should be returned to the sender. (back to 6.2.1)

**2-6 Security Evaluation & Censoring of all Public Disclosure**; This is the act of evaluating and preventing all unwanted public disclosure of information judged to be of strategic value to criminals. A security risk has been analyzed and a course of action to control it to an acceptable degree has been determined. When applied to sales literature, for example, the security risk might be the disclosure of technical information about a security end item that would be of strategic value. In this case, it would be expected that the specific literature making the disclosure would be removed from the public domain and/or passed on to third parties only after confirmation of their integrity. In this example, the technical information may or may not be legally covered by intellectual property rights either way it may still be of strategic value in helping a criminal to reproduce security end item properties. (back to 6.2.1)

**2-7 Secrecy Training;** This is teaching and testing the understanding of what must be treated as security sensitive, why they are sensitive, how unauthorized disclosure will be avoided and who can and cannot be made privy to security sensitive items and information. The teaching also means imparting an understanding of control methods such as the use of Non Disclosure Agreements, reporting of serious breaches and concealment from family members. (back to 6.2.1)

**2-8 Security Awareness Program**; Means that an organization's personnel shall be trained in basic security measures (password construction, virus protection and response, physical security, handling of protected information, etc.) and periodically reminded of their security responsibilities through means such as posters, flyers, or email communications. (back to 6.2.1)

**2-9 Visual Intrusion Barriers**; Are flexible or rigid surfaces having zero light transmittance at all wavelengths. (back to 6.2.1)

**2-10 Communications Monitoring;** This shall include systems for recording all incoming and outgoing phone calls, e-mails, faxes and cell phone calls. These systems must be able to record the incoming caller's identity and retrieve the calls, faxes and messages for a period of 6 months (back to 6.2.1).

**2-11 Centralized Call Receiving;** A system where all incoming calls are handled by one or more security trained persons who are able to screen calls and route them to security in the event of suspicion. (back to 6.2.1)

**2-12 Witnessed Meeting Procedure**; This is a written procedure for attendance at both internal and external meetings. The procedure ensures that two or more persons are witness to all transactions. (back to 6.2.1)

**2-13 Complete Destruction of Media**; The use of any process that converts media (i.e. documents, disks, et al) into a form that prevents reconstruction. (back to 6.2.1)

**2-14 Wire Tap Protection**; This is a system which detects and raises an alarm whenever a phone line is tapped. (back to 6.2.1)

**2-15 Use of False Data Trails**; A false data trail is the disclosure of false information aimed at thwarting acts of fraud The intentional use of false data by a business enterprise may be considered to be unethical. For this reason any business organization intending to use false data techniques, to thwart fraud, is advised to inform Law Enforcement to establish both efficacy and legality. (back to 6.2.1)

**2-16 Remote Listening System Evaluation**; A remote listening system is a highly directional microphone (or video camera for lip reading) which can be used at long range to listen to conversations and meetings carried out inside secure premises The intent of this requirement is to evaluate the potential for use of these techniques by unauthorized persons. It is not the intent that these techniques be used by a bona fide organization to eavesdrop on suspected fraudsters. (back to 6.2.1)

**2-17 Formal IT Security Risk Manager** – A person with the appropriate technical (IT) skills and who has formal responsibility for IT security risk management issues and approaches for the business. (back to 6.2.1)

**2-18 A Taking Work Home Policy;** A written specification of the terms and conditions under which personnel are permitted to remove either hard copy or computer files so that work can continue at/from home. (back to 6.2.1)

**2-19 Secure File Transfer Track & Trace**; This is a computer software sub system which provides a time history record of all users of secure data files and identifies the destination of all file duplication operations. (back to 6.2.1)

**2-20 Computer Access Control using Strong Passwords or other Strong Authentication Methods**; Strong Passwords means the use of a difficult to guess combination of letters and/or numbers to gain access to a secure data file. Strong passwords should also be no less than 7 characters in length , be changed at least every 90 days, and not be recycled. Other strong authentication methods may include biometrics, tokens, or digital certificates. (back to 6.2.1)

**2-21 Secure File Access Control**; Means that access to read, write, create or delete files is controlled based on the identity, role, or group of a user. This function will always be performed on those files deemed sensitive, such as confidential information or system files or directories. (back to 6.2.1)

**2-22 Secure External Data Transfer or Transmission**; Means the use of strong data encryption such as 3DES, AES, or other well known algorithms to encode sensitive, security-related information transferred or transmitted electronically or in physical media format to individuals or organizations who are external to the jurisdiction of the organizations IT security group. Such transmission includes the use of eMail, eMail file attachments and all forms of physical media such as optical discs, magnetic discs, flash memory etc.. (back to 6.2.1)

**2-23 Destruction of Media;** The use of any process that converts media (i.e. documents, disks, et al) into a form that makes reconstruction extremely difficult. (back to 6.2.1)

**2-24 Secure Wireless Transmission**; Wherever Wireless is used to connect to networks with protected information, the wireless environment must be secured using but not limited to methods such as changing default SSIDs, passwords, SNMP community strings, and strong enabling encryption such as WEP and WPA. (back to 6.2.1)

**2-25 Separate Web and File Servers;** Means where critical information or service is stored on run on a file server, any web server used to provide an interface for accessing this information must be secure and separated from the file server by a firewall. (back to 6.2.1)

**2-26 Laptop File Transfer Policy & Procedure;** A written specification of policy and procedure to be followed to ensure control over the use of portable electronic devices such as laptop computers or Personal Digital Assistants. The specifications must address both transfer of files to/from and creation and transmission of information of strategic value to criminals. (back to 6.2.1)

**2-27 Recordable Media Removal Policy**; A written specification of the policy and procedure to be followed to ensure control over the removal from secure premises of removable recording media such as floppy disks, hard disks, recordable CD's etc. (back to 6.2.1)

**2-28 Firewall on External Connection**; Means that anytime a network with confidential information is connected to the Internet or an untrusted 3rd party, the network shall be protected by a firewall. This means that the firewall shall log activity and that these logs shall be reviewed by an administrator on a regular basis (optimally daily), and that the firewall ruleset shall be reviewed on a regular basis and any unnecessary ruleset removed. (back to 6.2.1)

**2-29 Vulnerability Scanning**; Means that Internet-facing systems shall be probed on a periodic basis for security weaknesses. (back to 6.2.1)

**2-30 Password Reset Procedures**; Means there shall be a process to identify a user beyond a reasonable doubt prior to resetting lost or forgotten passwords. (back to 6.2.1)

**2-31 Computer Virus Protection**; Means that all systems that store, process, or have access to critical information shall be protected by anti-virus software. This includes any system that remotely access critical information, such as laptops. (back to 6.2.1)

**2-32 Security Patching**; Means that systems shall be kept up-to-date with the latest vendor security patches. Patches shall be installed in a timely manner. (back to 6.2.1)

**2-33 Account Lockouts**; Means a user account shall be temporarily disabled after a series of consecutive failed login attempts (typically 3 to 5 consecutive failed attempts). (back to 6.2.1)

**2-34 Physical Access Control of IT Systems;** Means facilities or data centers housing servers or networking equipment shall have controlled access limited to authorized personnel, and that visitors shall be identified via temporary badges, logged and escorted when provided access to IT systems. (back to 6.2.1)

**2-35 Track and Monitor Network Access**; Means access to IT systems shall be tracked through the use of system log files that captures pertinent data such as userID, source, date and time, system identity, and type of event and success or failure. (back to 6.2.1)

**2-36 Log and Review Critical Events**; Means that critical systems such as firewalls, routers, access points, IDS, shall log security events, and critical events shall be reviewed by an administrator on a regular basis. (back to 6.2.1)

**2-37 Maintain System Logs;** Means that a system log file shall be used that captures pertinent data such as user ID, source, date and time, system identity, and type of event and success or failure. (back to 6.2.1)

**2-38 Test Security Systems**; Means that the security mechanisms implemented by an organization shall be tested on a periodic basis. Examples include network penetration testing or testing of incident response plans. (back to 6.2.1)

**2-39 Incident Response Plan**; Means that the organization shall maintain a written plan for responding to security events. The plan shall include responsibilities, points of contact, incident scenarios, and procedures for responding to a security incident. (back to 6.2.1)

**2-40 Maintain a Current Network Diagram**; Means that a diagram showing all networks, systems, connections, firewalls, or WiFi access points shall be maintained and kept up to date. (back to 6.2.1)

**2-41 Change Control Process for IT Systems** Means that all changes to IT systems such as application or software updates, system patches, system additions or deletions, or application configuration changes, shall be done in a structured manner and approved by management. (back to 6.2.1)

**2-42 Remove Vendor Defaults**; Means that all systems shall be configured to remove default vendor accounts and passwords and modification of default security parameters such as SNMP community strings. (back to 6.2.1)

**2-43 Disable Unnecessary Services**; Means that all servers shall have services disabled which are not required for their function. For example, a web server that is installed by default shall be removed from a system that does not need to offer web services. In addition, insecure protocols such as rservices and telnet shall not be used. (back to 6.2.1)

**2-44A Strong Authentication for Remote Access**; Means that all access critical systems via the Internet or other remote means shall use a 2-factor authentication method based upon the principle of :-

a. Something you know (e.g. a strong password see NASPO 2-20)
b. Something you are (e.g. a biometric such as a fingerprint or voiceprint)
c. Something you have in your possession (such as but not limited to tokens or digital certificates).

(back to 6.2.1)

**2-44B Strong Authentication and Encryption for Remote Access**; Means that all access critical systems via the Internet or other remote means shall utilize strong encrypted connections such as a VPN, and shall use a 2-factor authentication as defined in NASPO 2-44A. (back to 6.2.1)

**2-45 Protect Backup Media**; Means that all backup media such as disks, CDs or tapes that store critical security sensitive information shall be protected from unintentional disclose through the use of methods such as encryption, labeling, physical tracking, accountability, and registered carriers for transport. (back to 6.2.1)

**2-46 Sanitize Media Before Disposal**; Means that electronic media such as disks, tapes, CDs, and hard drives should be either securely wiped using software that performs a multi-pass overwrite of the data, or shall be physically destroyed. (back to 6.2.1)

**2-47 Dual Secure Data File Access Control**; Means that two or more authorized persons must correctly identify themselves to the computer before access to a secure data file is granted to any one of them. (back to 6.2.1)

**2-48 Secure Data File Access Control using Biometric Measurement**; Means access that is personalized by the matching of stored biometric data with the matching input biometric data. (back to 6.2.1)

**2-49 Secure Data File Intrusion Detection System**; A combination of hardware and software processors that are able to detect all failed and successful attempts to penetrate Firewalls and other secure data file access barriers. (back to 6.2.1)

## A3 - Security Material Criteria Definitions

**3-1 Surveillance of Interior Secure Areas**; Deleted - see 5-15.

**3-2 Internal Secured Storage**; Designated secure areas within a facility that shall be controlled, through monitoring and access restriction, to a higher level than is commonly found within a facility. (back to 6.3.1)

**3-3 Restricted Access Areas**; Areas within a facility that are access controlled by various devices to restrict the entrance of unauthorized personnel. (back to 6.3.1)

**3-4 Incoming Inspection**; Inspection of materials received as to specification and count as compared to purchase requisition. (back to 6.3.1)

**3-5 Secured Disposal of Waste**; A procedure that ensures that security material waste is handled in such a manner that they are rendered unusable for the re-creation of a security product. (back to 6.3.1)

**3-6 Inventory Control**; An auditing process for the control of materials held in inventory. This process should track types of materials and their usage. (back to 6.3.1)

**3-7 Material Discrepancies Report**; A reporting and investigative device for incidents involving the loss or theft of materials. (back to 6.3.1)

**3-8 Vault Storage of Secure Materials**; Vault storage may be required for the control and safe keeping of selected, valuable security materials. (back to 6.3.1)

**3-9 Vault Storage of Finished Goods**; As a requirement, finished goods may need to be stored and or distributed from a secure vault area. (back to 6.3.1)

**3-10 Precise Accounting at Unit Level**; An auditing system by which materials can be controlled to a level of a single unit of measure. (back to 6.3.1)

**3-11 Written Cycle Counting Policy & Procedure**; An audit process that on a monthly or other periodic basis will perform a physical count on selected items and compared to the inventory shown in the business's computer system. The items selected shall be on a rotating basis and corrective actions must be defined for significant deviations of counted inventory. (back to 6.3.1)

**3-12 Multiple Signatures and Witnesses**; A system by which multiple signatures and witnesses are required for the receipt, dispensing and destruction of secure materials. (back to 6.3.1)

**3-13 Accountability of In-process Materials**; A system that can track the usage and production of security products during the manufacturing process. (back to 6.3.1)

## A4 - Supply Chain Criteria Definitions

**4-1 State/Federal confirmation of business**; This is either a state or federally issued valid business registration certificate. The certificate provided to the organization must correspond to the business which is seeking to purchase high security products from the organization. (back to 6.4.1)

**4-2 Written financial references**; A recognized independent financial report, such as a bank reference, a Dunn & Bradstreet (or equivalent) report or other disclosure from a recognized financial institution, that shows that the potential supplier is in good financial standing.
(back to 6.4.1)

**4-3 Written corporate references**; A written corporate reference is a letter or document issued by an independent third party corporation in favor of the potential customer. It is expected that this reference will state that the independent corporation has (over the previous 3 years) or is doing business with potential customer to the satisfaction of the third party corporation (back to 6.4.1)

**4-4 Written report by third party investigative agency re supplier of critical materials entity**; This is a report commissioned and paid for by the organization seeking Certification. The contents of the report are expected to indicate that the supplier of critical security material components or services is bona fide, and free from past and present behavior that are indicative of either fraudulent activity or security irresponsibility. (back to 6.4.1)

**4-5 Written confirmation that the ordering entity is authorized by the end-user to purchase the security feature**; Deleted - see NASPO 1-5. (back to 6.4.1)

**4-6 Written designation of authorized personnel**; In this case the writer must be either the Corporate Secretary or a senior executive of the potential or existing supplier. The written designation must identify those persons who have been authorized to decide and act on behalf of the potential customer on all matters related to the procurement of the accredited company's security product(s). (back to 6.4.1)

**4-7 Written document that demonstrates recognition of the need to control supply chain risks**; This must be a required company procedure. The document can be either a stand alone directive or a section in a more general company procedures manual. (back to 6.4.1)

**4-8 Signatures of understanding of the need to control supply chain risks from all personnel involved with security sensitive materials, devices, technology or information who interact with the supply chain.**; The signatures must be organized into record books to signify each individuals understanding and acceptance of the need to control supply chain risks. The record books must be treated as security documents, placed into secure storage when not in use and archived for several years when full. Entries into the record books must be restricted to authorized personnel only. To enhance the authenticity of signatures, biometric measures and electronic signatures may be appended to the basic signature of understanding. (back to 6.4.1)

**4-9 Documented track & trace for all shipments, including transportation, weight, quantity, trans-shipments, secondary shipments, and final application**; This data must be organized into record books and/or a secure computer data base. The record books and computer files must be treated as security documents, placed into secure storage when not in use and archived for several years when full. Entries into the record books and/or computer files must be restricted to authorized personnel only. (back to 6.4.1)

**4-10 Periodic third-party audits of compliance with documented procedures**; This must be a required company procedure. The third party audit procedure can be either a stand alone directive or a section in a more general company procedures manual The third party auditors must operate at arms length with the organization and have no conflicts of interest. (back to 6.4.1)

**4-11 Documented inspection of all incoming security materials**; The results of inspection (both quantity and quality) must be organized into record books. The record books must be treated as security documents, placed into secure storage when not in use and archived for several years when full. Entries into the record books must be restricted to authorized personnel only. (back to 6.4.1)

**4-12 Documented confirmation of security products end use**; This is a written statement signed by an authorized representative of the end user authority which clearly defines the end use of the security product. (back to 6.4.1)

**4-13 Documented procedures for actions to be taken when suspected breaches of security have been noted**; Deleted - see NASPO 8-2. (back to 6.4.1)

**4-14 Reciprocal Non Disclosure Agreements with Supply Chain Players**; Reciprocal means equal and opposite in the sense that the supply chain player is required to execute the same non-disclosure agreement with all third party organizations who supply the second party with any security components or services. (back to 6.4.1)

**4-15 Chain of Custody Policy with Distributors & Re-Marketers (D&RMs)**; In the context of security products, a custodian is a third party individual of organization at arms length having guardianship over the producers security products. A Chain of Custody Agreement (COC) is a legal agreement between the security product producer and custodian that defines the terms and conditions under which the custodian shall guard the producers security products. The COC agreement obligates the custodian to assure the security of the security products in accordance with an appropriate NASPO Class or it's equivalent. (back to 6.4.1)

**4-16 Written detail of Purchase ordering procedures**; These procedures apply both to orders placed by customers and suppliers of security materials or items. It is important to know that these orders have been officially sanctioned both internally and externally. The detail is intended to show what information flows back and forth in the process of completing the placing and acceptance of an order for security end items. (back to 6.4.1)

**4-17 Secured storage for all Purchase requisition/authorization, whether hard copy or electronic, documents**; Secured storage means that access to the storage area (whether a vault, safe, cabinet or computer file) is restricted to formally authorized personnel who have been security cleared by the potential customer. (back to 6.4.1)

**4-18 In-house audit procedures to confirm compliance with documented procedures**; This must be a required company procedure. The audit procedure can be either a stand alone directive or a section in a more general company procedures manual. (back to 6.4.1)

**4-19 Contract/document specifying product use rules**; Product "Use Rules" specify the terms and conditions for use of the security product or technology by the customer.. (back to 6.4.1)

**4-20 Written report by third party investigative agency re firms to which security products will be supplied**; This is a report commissioned and paid for by the organization seeking Certification. The contents of the report are expected to indicate that the firms to which security products will be supplied are bona fide, and free from past and present behavior that are indicative of either fraudulent activity or security irresponsibility. (back to 6.4.1)

**4-21 Written confirmation by regulating agency**; In this case, the regulating agency has been cited by the potential customer as the end-user of the Security Product to be supplied by the potential customer. Preferably in written form, this is confirmation by the regulating agency (usually an issuing authority or governmental agency) that the supply contract claims of the potential customer are true. (back to 6.4.1)

**4-22 Verifiable signatures/passwords for authorized personnel**; Verifiable signatures are exemplars of the hand written signatures of all personnel who the potential customer has notified in writing will decide and act on it's behalf in all matters related to the procurement of the Accredited Organization's security product(s). The passwords used shall enable the Accredited Organization to know the identity of the person who has sought access to the password controlled system. (back to 6.4.1)

**4-23 Second person review of all orders/shipments**; This must be a required company procedure. The audit procedure can be either a stand alone directive or a section in a more general company procedures manual. The second person, like the first, must be knowledgeable with respect to customer validation and secure shipping procedures. The second person must have no conflict of interest with the first person and must carry out independent reviews. (back to 6.4.1)

**4-24 Inspection/audit of facility to which security products are shipped to ensure security compliance**; This audit should preferably be carried out by an independent

Auditor or NASPO Auditors to NASPO Standards. The audit must culminate in a written statement of compliance which indicates how compliance was verified. (back to 6.4.1)

**4-25 Transportation Assurance when Security Sensitive Goods are Sold FOB the Supplier's Shipping Dock;** Transportation assurance requires the shipper to verify the identity of the person(s) receiving goods for transportation, to confirm authenticity and authorization and requires the shipper to obtain confirmation of successful delivery to the end user or customer. (back to 6.4.1)

**4-26 Transportation assurance procedure**; A procedure used by shipping and receiving personnel to enable suppliers and customers to know without doubt that :-

1) security sensitive goods shipped have been picked up by personnel authorized by the customer or end user.
2) security sensitive goods shipped have been transported to their destination by means approved by the customer or end user.
3) security sensitive goods have arrived successfully at their destination.
4) change of ownership of security sensitive goods will not cause a lowering of security assurance.
5) at all times one or more organizations are actively involved in the security assurance of the security sensitive goods.

Organizations who can show that they are in compliance with the latest Transported0 Asset Protection Association (TAPA), Freight Security Requirements (FSR) will be considered to be in compliance with this requirement.
(back to 6.4.1)

## A5 - Physical Intrusion Criteria Definitions

**5-1 Exterior Surveillance**; Use of Closed Circuit security camera(s) that is/are mounted on the exterior of a building to monitor access points and areas of concern. Images from these cameras must be retained and be reproducible for a minimum period of 90 days after the recording is made. (back to 6.5.1)

**5-2 Controlled Access Exterior Doors**; Exterior doors must contain an automatic locking device that restricts the entrance of unauthorized persons, but provides for controlled access of authorized personnel. Alternative ways may be used to detect and control unauthorized access provided that they are equally effective. (back to 6.5.1)

**5-3 Alarmed Entrances**; Exterior entrances that provide an alarm either audible or to a monitored system when doors are opened by unauthorized persons. (back to 6.5.1)

**5-4 Alarmed Emergency Exits**; Emergency exits that are equipped with a device that provides an audible alarm when doors are opened. (back to 6.5.1)

**5-5 Exterior Lighting**; Lighting must be maintained to a minimum level on exterior areas of the building, in particular, access areas and areas of concern. (back to 6.5.1)

**5-6 Secure Exterior Walls**; The exterior walls of the facility should be of such a material that would provide a significant level of difficulty to attempts of intrusion. (back to 6.5.1)

**5-7 Monitored Exterior Windows**; Windows on the exterior of a facility should be monitored by devices that can readily detect unauthorized entry or breakage. The detection devices should be monitored by security personnel. (back to 6.5.1)

**5-8 Controlled Roof Access**; All roof access doors must be secured with devices that prohibit unauthorized entry. Controls should include locks and alarm monitoring devices. (back to 6.5.1)

**5-9 Physical Perimeter Barriers**; Security fences and gates should provide a significant barrier to unauthorized access to the facility. The intent of this barrier should be to delay any attempt of intrusion to an extent that security and/or law enforcement personnel can respond. Gates and fences are typically monitored or controlled. (back to 6.5.1)

**5-10 Guard Monitored Perimeter**; A trained uniformed guard shall monitor the perimeter of a facility through the use of electronic surveillance or line of sight observation. (back to 6.5.1)

**5-11 Main Entrance Controlled Access**; The main entrance of the building shall be controlled by access control devices and interlocking door devices monitored and activated by security personnel or receptionist. (back to 6.5.1)

**5-12 Visitor Access Control & Recording**; Visitors are defined as all persons who have not been formally issued with an access credential either in the form of an access ID card and/or their identity made known to a security guarding function. Access will normally be denied if the person is unknown to the security guard or the personalized access control system fails to authenticate the card and/or person if a biometric system is used. Recording means that the identity of all persons gaining access must either be automatically recorded by the automated access control system or noted by the guard. The record must indicate the time and point of access. (back to 6.5.1)

**5-13 Internal Secure Areas**; Designated secure areas within a facility that shall be controlled, through monitoring and access restriction, to a higher level than is commonly found within a facility. (back to 6.5.1)

**5-14 Vault Area**; The vault is the primary security storage area in the facility. It is typically isolated from outside walls, constructed of reinforced concrete, dual access control systems, and heavily monitored and alarmed. (back to 6.5.1)

**5-15 Interior Surveillance**; Through the use of closed circuit cameras the interior secured areas of a facility shall be monitored through the use of continuous recording devices and/or monitoring by security personnel. (back to 6.5.1)

**5-16 Waste Destruction Area**; A designated area for the destruction of security material, this area should be monitored by CCTV or under dual control. (back to 6.5.1)

**5-17 Motion Detection**; Devices used in secure areas to detect the movement of persons in the area. When armed the devices should provide an alarm to security or monitoring personnel. (back to 6.5.1)

**5-18 Fire and Smoke Detection**; Smoke and fire detection devices should be installed throughout the facility and monitored on a continual basis. (back to 6.5.1)

**5-19 Internal Emergency Alarm System**; This system falls within the organization's secure premises. The system enables a person who is under duress inside the premises to add, inconspicuously, a special code which raises an alarm. The special codes can be added to both physical access terminals and computer file access protocols. Duress alarm buttons are typically provided at common entrance areas, secure areas, vaults, and security control rooms. They are typically monitored both internally and externally. The activation of a duress button should have a required response time from the monitoring service. Any use of a duress button should always be recorded. (back to 6.5.1)

**5-20 Restricted Access Areas**; Areas located within a facility that restrict the entrance of unauthorized personnel. (back to 6.5.1)

**5-21 Controlled Shipping and Receiving**; Dock areas must include devices and barriers that restrict the movement of transportation personnel to designated areas. These devices and barriers shall provide for a physical separation and visual obstruction of secure areas from dock areas. (back to 6.5.1)

**5-22 Guard Controlled Access**; At points of common entry a trained uniformed guard shall control the access of all personnel entering and exiting the facility. (back to 6.5.1)

**5-23 Security Control Room**; If a security control room (SCR) is used it must be an enclosed and restricted area containing monitoring and control devices for the facilities security. This room may also accommodate security personnel. Access to the security control room must be locked at all times with limited access and records of access/egress. Entry should be on a "need to be there" basis and approval for access must be reviewed by Security Management. The intrusion resistance, surveillance and access control of this room of this room must comply with NASPO 5-13, 5-15 and 5-20 respectively. (back to 6.5.1)

**5-24 Dual Control Access**; In designated secure areas, entrance can only be made with a minimum of two people; typically a minimum of two people must be in the area any time the area is occupied. (back to 6.5.1)

**5-25 Dress Codes for Restricted Areas**; A dress code that reduces the possibility of secure products being easily concealed and stolen. These usually encompass the use of pocket-less garments and a restrictions of items that can be taken into and out of a secure area. (back to 6.5.1)

**5-26 External Emergency Alarm System**; This system is used outside of the organization's secure premises. The system enables a person under duress away from the secure premises to transmit a special code which raises an alarm and transmits the person's identity, time, date and location. (back to 6.5.1)

**5-27 Key Controls**; Procedures and practices that ensure that all facility access keys or control devices are restricted to usage only by authorized personnel. The procedures should track the issuance of all facility keys and provide for a response to the loss or unauthorized use of those keys or devices. (back to 6.5.1)

**5-28 Vault Combination/Key Controls**; The combination/key to the vault must be strictly controlled through procedures that ensure that unauthorized access is prohibited. (back to 6.5.1)

**5-29 Remote Monitoring Media Control**; A system must be in place to secure and archive security media (i.e. computer disks, video tapes, et al). The appropriate length of storage time shall be in relationship to the products being produced, but typically not less than three months. (back to 6.5.1)

**5-30 Policies, Procedures and Preparedness for the Management of Physical Intrusion**; The policies, procedures and preparedness of the organization must be comprehensive and include all forms of intrusion.. (back to 6.5.1)

**5-31 Deleted – see NASPO 5-30**

**5-32 Deleted – see NASPO 5-30**

**5-33 Security System Back Up Power Supply**; In the event of an interruption of power, a back up power source must be maintained to support the facilities security systems. (back to 6.5.1)

**5-34 Access Control Monitoring**; A monitoring device by which a determination can be made as to the identity of the individuals entering or leaving a restricted area through an access point. (back to 6.5.1)

**5-35 Deleted – see NASPO 5-30**

**5-36 Prevention of Unauthorized Multi Person Access (commonly known as "piggy backing") to Secure or Restricted Areas using the Identity and Access Permission of a Single Person**; A physical door or entrance system that makes it extremely difficult for two or more persons at the same time to enter a secure or restricted area based upon access permission granted to a single person. (back to 6.5.1)

## A6 - Personnel Criteria Definitions

**6-1 Employee References**; The evaluation, often conducted during the employment screening process, made to determine the accuracy of employment information provided by the potential employee. (back to 6.6.1)

**6-2 Credit Check**; Data related to the credit ratings of personnel must be obtained from one or more independent, recognized credit bureau's or agencies and evaluated by security management of the organization to determine whether personnel security risks exist from significant financial debt or mismanagement. (back to 6.6.1)

**6-3 Criminal Records Check**; Data on the criminal history of employees must be obtained from an independent, recognized agency with the resources to access criminal records held by various governmental authorities. Organizations seeking security assurance certification must then evaluate this data to determine whether personnel security risks exist as a result of an employee's prior criminal history. (back to 6.6.1)

**6-4 Drug Screen**; Tests on existing or potential new employees must be carried out by a qualified medical laboratory to screen for drug or substance abuse. Test results must then be evaluated by the organization to determine if the use of any drugs (that may be illegal or effect performance) are likely to present a security risk. (back to 6.6.1)

**6-5 Social Security Number Verification**; This is the process of verifying, via use of the Social Security Administration data base, that a person is the rightful owner of the social security number that he/she has revealed to the organization. This requirement shall apply to all existing employees who are privy to security sensitive information or who perform security sensitive jobs or tasks as well as prospective new employees.

**6-6 Annual Credit Check**; This is a repeat of the background check defined in 6-2 carried out on the anniversary of background check. The purpose of the annual check is to look for early warnings of potential problems and signs of instability in an individual which may require corrective action. (back to 6.6.1)

**6-7 Motor Vehicle Violations**; A search by a responsible agency is made to determine the amount and type of motor vehicle violations of a potential or existing employee. This requirement is especially applicable to employees who handle motorized vehicles for the purpose of transporting security sensitive goods or materials. (back to 6.6.1)

**6-8 Formal Education**; In the case where formal education requirements are a prerequisite for employment or promotion, verification must be made to the educational institution to validate information provide by the individual. (back to 6.6.1)

**6-9 Fingerprint Screen**; Fingerprints of potential employees shall be screened by a responsible agency to determine the identity of the individual, any potential criminal risks, or existing criminal records. (back to 6.6.1)

**6-10 Fingerprinting**; In those States and Provinces where fingerprinting is legal, a full set of legible fingerprints of employees involved with security products, and any additional personnel deemed necessary shall be maintained on file. (back to 6.6.1)

**6-11 Photograph**; A current photograph (usually every 3 years) of each employee shall be maintained on file. (back to 6.6.1)

**6-12 Employee Security Policy**; This is a document provided to the employee detailing security risks, responsibilities, procedures and disciplinary policies for which each employee must be knowledgeable. (back to 6.6.1)

**6-13 Company Security Policy**; A policy, typically of a confidential nature, that prescribes all the policies and procedures that pertain to security issues within the organization. (back to 6.6.1)

**6-14 Annual Employee Security Training**; Security training should be provided in conjunction with the employee security policy to ensure that security practices are understood and consistently implemented throughout the organization. These training sessions must be conducted upon hire for all Classes, as well as once annually for Class II and twice annually for Class I. After hiring, reading the employee security policies and training, all Classes must require the new hire to signify understanding and acceptance of the security requirements by signing a letter of understanding.
(back to 6.6.1)

**6-15 Security Management Responsibility**: This is a knowledgeable individual or TEAM of individuals shall be designated as having responsibility for organizational security. The duties and responsibilities of this individual are typically detailed in the company Security Policy. (back to 6.6.1) Where a team of individuals manages the business security system, a method for integrating their approaches and decisions needs to be practiced.

**6-16 Security Guard Policies and Procedures**: This is a set of policies and procedures detailing the use and administration of all security guards if and when their services are required. This policy is typically a part of the company Security Policy. (back to 6.6.1)

**6-17 Use of Internal Security Awareness Communications;** Security awareness communications are eye catching visual displays that serve to remind personnel of their security responsibilities or bulletins that provide personnel with security updates. (back to 6.6.1)

**6-18 Psychology Testing / Screening**; A psychology exam may be required in certain positions to determine the security risk of the individual. (back to 6.6.1)

## A7 - Disaster Recovery Criteria Definitions

**7-1 Plan for Securing Facilities**; This plan details the basic requirements for securing a facility in the event of a security breakdown, by either manmade or natural events. (back to 6.7.1)

**7-2 Data and Information Security Plan**; This is a document prescribing how information and data will be maintained in a secure environment in the event of a breach in security. The breach may be created by either manmade or natural causes. (back to 6.7.1)

**7-3 Use of Armed Personnel in the Event of Disaster**; This Is a written policy for the restoration of security in the event of a breakdown following either a manmade or natural disaster. The policy must detail the use and control of armed uniformed personnel for the protection and maintenance of security. This requirement does not mandate the use of armed personnel following a disaster. The decision to do so remains the responsibility of the affected organization. (back to 6.7.1)

**7-4 Chemical/ Biological Incident Plan**; This policy shall detail the procedures that will be implemented in the event of a hazardous chemical or biological incident. Those procedures will focus on the maintenance of security levels to prevent the loss of control of products and materials. (back to 6.7.1)

**7-5 Terrorist/Armed Intruder Attack Plan**; This plan of action details the organizational response to an attack by Terrorist or Armed Intruders. (back to 6.7.1)

**7-6 Use of Uniformed Personnel in the Event of Disaster**; The policy should detail the use and control of unarmed uniformed personnel in the event of disaster for the protection and maintenance security. This disaster may be either a manmade or natural event. (back to 6.7.1)

## A8 – Security Failure (Breach) Criteria Definitions

**8-1 Security Breach Incident Log**; This is a written record of all breaches of security. The record must give time and date, a brief description of the breach and the area of risk that is most appropriate. An analysis of cause and effect may also be included. (back to 6.8.1)

**8-2 A Written Breach Handling Procedure**; A procedure that details what happens when there is a breach of security. (back to 6.8.1)

**8-3 A Designated Breach Manager**; This is the person made responsible for causing the organization to follow the Breach Handling Procedure and successful completion of necessary corrective actions. (back to 6.8.1)

**8-4 Failure Modes & Effects Analysis of Selected (Critical Only) Security systems**; This is an analysis limited to the most critical security systems whose failure is judged, in advance, to have serious consequences. Failure Modes & Effects Analysis examines what happens when systems set up to control security risks, fail. This type of analysis creates failure scenarios and then determines their effects and consequences. This type of analysis is used to set control priorities and to determine ways to mitigate fraudulent acts if and when they occur. (back to 6.8.1)

**8-5 Plans & Preparations for Recovery & Mitigation of Effects**; These plans define how the organization will react to fraudulent acts, recover from them and mitigate their effects by preserving the intrinsic security value of the NASPO Members security products. (back to 6.8.1)

**8-6 Company & Employee Legal Liability Awareness**; This is a combination of briefings and written material which impart (to all personnel) an awareness of the consequences of security failures. (back to 6.8.1)

**8-7 Links with Crime & Intelligence Agencies**; Are contacts who agree to provide early warning of possible fraudulent acts or trends related to the security products of the company. (back to 6.8.1)

**8-8 Historical Breach Experience Reports**; These reports provide a precise account of each breach of security, how and why it happened, the after effects and corrective actions taken. (back to 6.8.1)

**8-9 A Critical Security Area Video Monitoring system**; This is a CCTV system which enables security guards to clearly view and make time history records of activities in high security areas. (back to 6.8.1) (back to Table of Contents )

**8-10 Security Breach Informing System (Ears & Eyes)**; This is a procedure to encourage organization personnel to always be on the lookout for and report significant breaches of security. Those reported must be logged, analyzed and acted upon to prevent a reoccurrence. (back to 6.8.1)

**8-11 A Working Relationship with Law Enforcement**; The existence of a working relationship with local law enforcement to gain agreement to work together to detect, control, and respond in a timely manner to fraudulent acts related to the security products of the company. (back to 6.8.1)

**8-12 A Comprehensive Failure Modes & Effects Analysis**; This is an analysis of the entire security systems in the event of failure. Failure Modes & Effects Analysis examines what happens when systems set up to control security risks fail. This type of analysis creates failure scenarios and then determines their effects and consequences. This type of analysis is used to set control priorities and to determine ways to mitigate fraudulent acts if and when they occur. (back to 6.8.1)

**8-13 Links with Interpol**; May be direct or via local law enforcement. The purpose of the link up is to enable use of Interpol's compendium of relevant security feature exemplars, fraudulent simulations and fraudulent techniques. (back to 6.8.1)

**8-14 Automated Material Track & Trace system**; A system that is able, without human intervention, to provide information on demand of where physical security sensitive items are, where they have been and possibly where they will be in the future. As a minimum, the scope of this system will include items internal to the organization and items that are upstream and downstream in the supply chain. Internal items shall include those entered into the inventory and on the shop floor. (back to 6.8.1)

**8-15 A Personnel Track & Trace system**; This is a time history record of the location and possible activities of all personnel. The record should extend back in time a minimum of 6 months. (back to 6.8.1)

**8-16 A Document Track & Trace system**; This is a time history record of the location of security documents of potential strategic value to criminals. The record should extend back in time a minimum of 6 months. (back to 6.8.1)

## A9 – Security Risk Management Related - Criteria Definitions

**9-1 Perform Security Risk Management;** To comply with ANSI/NASPO security assurance requirements the organization must practice and perform the functions of security risk management to a degree that is satisfactory and sufficient to meet the stated objectives and comply with all risk reduction requirements in this area. General guidelines for the performance of security risk management functions can be found in NIST Special Publication 800-30 at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf , NIST Special Publication 800-100 at http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf and ISO 27001.

**9-2 Identify & Classify all Security Sensitive Physical and Information Items;** Identification is knowledge of those physical and information items that must be treated by the organization as security sensitive – and hence protected. Classification is a process of further evaluation that results in the security sensitive physical and information items being categorized, as a minimum, into those that are highly security sensitive (critical) and those that are less critical. This identification and classification must be communicated to NASPO in the form of a pre-audit deliverable.

**9-3 Perform Security Threat Identification & Analysis;** A security threat is a potential cause of an unwanted incident, which may result in unauthorized possession of physical security sensitive items or information. The potential causes of these unwanted incidents must be identified and an analysis of them carried out to determine their source and likely form of manifestation. These findings must be communicated to NASPO in the form of a pre-audit deliverable.

**9-4 Perform Security Vulnerability Identification and Analysis;** A vulnerability is a weakness in the security net (measures) of the organization that can be exploited by one or more threats. These weaknesses must be identified and an analysis of them carried out to determine their likelihood of being exploited by the threats and what the consequences of exploitation are likely to be. These findings must be communicated to NASPO in the form of a pre-audit deliverable.

**9-5 Perform Security Risk Identification, Analysis and Assessment;** Risks are the likelihood of the consequences resulting from the security threats exploiting the security vulnerabilities. The likelihood of consequences occurring must be identified and an analysis of them carried out to determine whether or not the organization is taking risks by virtue of having no or ineffective risk reduction countermeasures to them. These findings must be communicated to NASPO in the form of a pre-audit deliverable.

**9-6 Designated Security Manager;** A knowledgeable individual or team of individuals shall be designated as having responsibility for organizational security. The duties and responsibilities of this individual are typically detailed in the company Security Policy. Where a team of individuals manages security risk, a method for integrating their approaches and decisions must to be practiced.

**9-7 Designated IT Security Risk Manager;** A person with the appropriate technical (IT) knowledge and skills and who has formal responsibility for IT security risk management issues and approaches.

(back to Table of Contents )

**The balance of this page is intentionally left blank.**

# APPENDIX B - Background & Legalities

## I) Background

The Security Assurance Standards of the North American Security Products Organization are based upon a need within the industry to bring a higher level of security and risk recognition to the industry. The concern for security products within North America has traditionally lagged behind other parts of the world. This has been a contributing factor to a high level of both document, issuance and product fraud and a degradation of the value of security technologies and services. To counter this increasing problem, and to bring a higher level of recognition to the risk and responsibilities of security product production, a standards development and certification organization was created.

The North American Security Products Organization was formed by people within the document, issuance and product security industries who recognized the urgent need to tackle the fraud issues facing those industries. These people looked at the examples provided by various countries, organizations and industries faced with similar fraud issues. Those examples exhibited a history, culture and structure of security product production not commonly found within North America. Some of those organizations had developed structures to control the security technologies, production of products and issuance of end items. These controls are based upon risk reduction standards and the capability to audit and certify organizations to those standards. Since there was no existing organization within Canada and the United States to develop these standards and audit and certify organizations, NASPO set this task as its priority.

A committee of the NASPO board of directors has developed, with the participation of interested parties, a set of auditable standards that establish criteria to reduce the risks involved in the production of security products and their related technologies and services. This committee identified eight areas of critical security risk; Customer Related, Information, Material Control, The Supply Chain, Physical Intrusion, Personnel, Disaster Recovery, and Security Failure Risk (in a subsequent review, a ninth area, concerning the risk of improperly performing risk management, was added to this version). The committee acknowledges that risks can be reduced in various acceptable ways. So, in developing the standards, a degree of flexibility is incorporated with the use of “enhancement” or optional criteria in each risk management category. The standards do recognize numerous accepted solutions and practices. Organizations will be audited using these standards of solution as the basis of security assurance quantification and determination of classification.

This document details the consensus standards and conformity assessment systems that were developed.

Industry, public, and governmental input to the standards is welcome and solicited. Please address your suggestions to; The NASPO National Standards Committee, e-mail; nnsc@naspo.info, or call (202) 587-5743

## ii) Development and Use of Standards

The security standards presented in this document are based upon input received from members of the North American Security Products Industry combined with the consensus process. Risk reduction was used as the basis for development of the standards criteria.

The standards have been presented to interested supplier and end user organizations for their review and input. This process of review was used to reach a consensus. As a result, substantial agreement has now been achieved by the interested parties. Unanimous agreement is not a requirement. Review and approval by the NASPO National Standards Committee, NNSC (the NASPO standards body recognized by ANSI) was, however, a requirement for the issuance of these standards.

The Risk Management approach has been taken because many ways exist to control the same risk. Ways that work for one organization operating at one level of security may not work for another at a different level. The risk (or problem), however, is the same in both cases but controlling it to the Class I Standard may require a different approach and much higher investment in infrastructure and systems.

As time goes on it is expected that new forms of threat to anti fraud products and services will emerge. When this happens NASPO plans to update this risk definition document and re-issue it to enable all Stakeholders to keep on top of the challenges as they emerge.

The purpose of the standard is to;

a. Define the critical risk factors.
b. Recognize and if necessary improve upon industry accepted risk reduction techniques.
c. Provide a method of assessing the value of each risk reduction technique.
d. Allow a trained auditor to objectively evaluate the security classification of an organization.
e. Provide an organization with a guide to acceptable security practices.
f. Enable an end user to objectively identify the security practices required by their own products and services.

In creating this standard every effort has been made to allow organizations the latitude to develop and adopt security procedures and techniques that best match their required needs. It is also recognized that each organization may have different security requirements based on the products and services they provide. The standards attempt to recognize those differences. But, to be recognized as NASPO Certified, a minimum standard must be met using industry accepted risk reduction techniques.

It is specifically <u>not</u> the purpose of the standards:

a. To endorse various anti fraud devices or systems offered by a manufacturer.
b. To evaluate the value or security worthiness of individual security devices, technologies, services or products.
c. To recommend one security product producer or service provider over another.
d. To assess the quality, production capability or service level of an organization.

The use of the standards is voluntary to non-certified security product producers and non members of NASPO.

The certification process is based upon the voluntary implementation of risk reduction infrastructure, systems and procedures followed by a mandatory audit by trained and certified NASPO auditors or commercial certification bodies accredited by NASPO.

### iii) Determination of Certification Class

NASPO will make no determination of the level of security and therefore class of certification required for individual products, services or organizations unless a NASPO auditor believes that a major mismatch exists between the class applied for and level of security assurance that should accompany a specific security product or service. Analysis of vulnerability, security risk, the establishment of organizational standards of risk reduction and choice of the means to accomplish it will remain the responsibility of the individual organizations in spite of requiring, in Section 6, that minimum risk reduction methods must exist to achieve a desired class of certification. For more information concerning this NASPO policy, please refer to the audit process in Section 7.0.

### iv) No Restriction of Trade

Under no circumstances shall these standards be implied as a restriction of trade. The lawful right of free enterprise will prevail regardless of NASPO certification.

### v) Right of Revision

This set of standards issued by the North American Security Products Organization may be revised or revoked at any time. The standard must be reviewed in its entirety by the NASPO National Standards Committee (NNSC) every two years. Any revision or revocation of standards carried out by this consensus body must be in accordance with 'NASPO Procedures for Development of American National Standards' approved by ANSI (goto : www.naspo.info/pages/sdoprojects.html to down load a copy) Participation in the review and update of this standard is open to all stakeholders. To participate in this consensus process please goto : www.naspo.info/pages/sdoprojects.html and register your stakeholder interest.

### vi) Right of Appeal

For all classes of certification there shall be a right of appeal following the submission of an auditors report and certification review by the NASPO Certification Committee. All appeals and protests shall be in accordance with NASPO Audit Procedure No.1.

### vi) Bi-Annual Review and Update

Following procedures for development of American national standards approved by ANSI (goto : www.naspo.info/pages/sdoprojects.html to down load a copy) a full review of the original standard issued in 2005 as ANSI/NASPO-SA-v3.0P-2005 was carried out in 2007/2008 under the auspices of the NNSC and issued as ANSI/NASPO-SA-2008. This revised version is the result of the 2007/2008 review by the NNSC.

(back to Table of Contents )

**The balance of this page is intentionally left blank.**

NASPO
NORTH AMERICAN SECURITY PRODUCTS ORGANIZATION

# Appendix C

## Audit Application
## &
## Self Assessment Form

**This document will be provided at the time of Application for NASPO Certification**

**Version 1.0**
**August 19, 2003**
© NASPO 2003

**1425 K Street, NW, Washington, D.C. 20005, U.S.A.**
**www.naspo.info**

# APPENDIX D - GLOSSARY

## A

***access control;*** to restrict the right or ability to log on to a computer system or retrieve information from a computer

***acquire;*** to come into possession, control or power of disposal of often by some uncertain or unspecified means

***AES;*** in cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the US government. It is expected to be used worldwide and analyzed extensively, as was the case with its predecessor, the Data Encryption Standard (DES). AES was adopted by National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001 after a 5-year standardization process

***anti-virus software;*** computer software that consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software

***applicability;*** how relevant the risks are to the organization being audited

***audit report;*** a document detailing the findings of an audit

***audit trails;*** a chronological record of when users log in, how long they are engaged in various activities, what they were doing, whether any actual or attempted security violations occurred.

***audit;*** a systematic check or assessment, especially of the efficiency or effectiveness of an organization or department, typically carried out by an independent assessor and concluding with a detailed report on findings.

***authentic security products;*** products having a claimed and verifiable origin or authorship; not counterfeit or copied

***authentication****; a process that shows something to be valid or true*

***authority;*** somebody or something with official power to enforce rules or give orders

## B

***background checks;*** a process in which the specifics of an individual's past history are revealed for the purposes of employment or obtaining classified information

***backup media;*** products used to store a copy of electronic files (i.e., tapes, removable hard discs, cds, dvds

***backup operation;*** capability that has been deliberately introduced and exists to enable failed or malfunctioning operations to be restored to a normal operating condition or degraded state of operation on a temporary basis. In both cases the goal of the backup capability is to enable the operation to go to successful completion

***barrier;*** an obstacle that prevents movement or access

***benefit;*** something that creates an advantage

***best practices;*** planning or operational practices that have proven successful in particular circumstances

***beyond a reasonable doubt;*** that there is no manner of doubt

***biometric access control;*** any means of controlling access through human measurements such as fingerprinting, voice printing and iris recognition

***bona fide;*** honest and sincere of intention

## C

***cartel;*** an alliance of independent private enterprises formed to control production, price and distribution of a commodity or service

***CDs;*** compact discs; a small optical disc on which data such as music, text or graphic images is digitally encoded

***chance of success;*** the likelihood of achieving what is planned or attempted

***change control processes;*** procedures and practices that ensure that changes made to a design, practice , procedure, method etc, are not implemented without prior review approval and authorization

***circulation;*** dissemination of something among end users

***circumvent;*** to find a way of avoiding restrictions imposed by a rule or law without actually breaking it

***clearance;*** permission to do something or for something to take place

***code of practice;*** a set of rules for or standards of professional practices or behavior set up by an organized group

***complete systems;*** security products and services having all of the necessary or appropriate parts

***components;*** a part or element of a larger whole

***comprehensive information security policy;*** a complete program of actions adopted company-wide towards protecting information available on the network

***computerized personal data;*** recorded information about persons

***confidentiality agreement;*** a contract whereby one party can disclose secret information to a second party without losing control over the secret information

***contents;*** the topics, ideas, facts or statements contained in a document

***control systems;*** a set of interconnected components that normally include a measurement device, a device to compare the measured quantity with a required quantity a decision device that changes the measured quantity towards the required quantity and continues to do so until the measured and required are the same.

***counterfeit resistance;*** the degree of difficulty involved in creating a perfect mimic of something.

***countermeasures;*** a measure or action taken to counter or offset another one

***credible forms of fraudulent action;*** convincing, believable examples of actions that are dishonest, untrue, or unfair, and intended to deceive people

***credit;*** a measure of recognition that an organization has fulfilled a requirement

***criminal intent;*** the design or purpose to commit any wrongful or criminal act

***critical components;*** a necessary part of the product

***critical data;*** data that is very sensitive or important

***critical security components;*** parts of a security product that are crucial to its performance

***custodian;*** each individual or company in possession of the product on its way to the final end user

***custody;*** to be in possession of a product at a given time

## D

***data package;*** a collection of data either in the form of multiple documents or computer files.

***deception;*** to deliberately mislead into believing something false

***degree;*** amount, level or extent

***delivered;*** provide what is promised or expected

***demonstrate;*** to show or prove something clearly and convincingly

***DES;*** DES is an acronym for Data Encryption Standard. It was originally developed by IBM as Lucifer in the early 1970's. The NSA and NIST used a modified version of Lucifer and named it DES. DES was adopted as the federal standard in 1976 (FIPS (46-3) and ANSI standard X9.32). However, DES became vulnerable as computers got more powerful and simple DES is no longer secure and has been cracked. So NIST defined 3DES or Triple DES in 1999. 3DES uses three stages of DES so it is much more secure and suffices for most applications currently. In 2001, NIST replaced DES by AES (Advanced Encryption Standard). It is hoped that AES will remain strong enough for the next 10-20 years.

***3DES;*** DES is a block cipher - i.e. it acts on a fixed-length block of plaintext and converts it into a block of ciphertext of the same size by using the secret key. In DES, the block size for plaintext is 64 bits. The length of the key is also 64 bits but 8 bits are used for parity. Hence the effective key length is only 56 bits. In 3DES, we apply 3 stages of DES with a separate key for each stage. So the key length in 3DES is 168 bits. Decryption is done by applying the reverse transformation to the block of ciphertext using the same key. Since the same key is used both in encryption and decryption, DES is a symmetric key cipher. This method differs from algorithms like the RSA encryption which use different keys to encrypt and decrypt a message.

***deterrent;*** to prevent or discourage someone from doing something by making them fearful of the consequences or by making it too difficult for them to achieve their goal

***disclosure***; exposure, to make secret information known

***distributors & re-marketing organizations;*** organizations that are neither the source or sink of security products or technologies or services. Intermediaries who distribute and re-market a security product manufactures by another organization. Distributors are normally sales agents of the producer. Re-Marketers often operate under their own brand name and sometimes add some form of extra value to the product prior to re-sale.

***document;*** a formal piece of writing that provides information or acts as a record of events or practices

***due diligence;*** the care a company should take before entering in an agreement or transaction with another party

## E

***effective;*** causing the desired or intended result

***electronic files;*** organized data stored in a computer

***electronically transmitted;*** an exchange of information via internet, e-mail or FTP sites

***employment screening;*** the initial evaluation of an individual intended to determine suitability for a company, often includes criminal record check, qualifications verification, credit rating, etc.

***end users;*** a person or group that is one of the ultimate consumers or users that a product has been designed for

***enhance;*** to increase the degree of detail with regard to security assurance practices

***enterprise;*** organized business activities

***exemplars;*** an representative that serves as a pattern

***extent;*** the degree to which security assurance practiced

## F

***fail operational;*** a failure that does not result in loss of operational capability. Continued operation, following a break down or malfunction, is usually enabled by either an automatic or operator initiated backup system.

***falsification of documents;*** the deliberate act of making alterations for the purpose of committing fraud.

***firewall;*** a system or combination of systems that enforces a boundary between two or more networks

***firewalling internet connections;*** installing a firewall on all internet connections

***floppies;*** floppy disc; a flexible plastic disc coated with magnetic material and covered by a protective jacket, used primarily by computers to store data magnetically (also called *diskette*)

***forensic evidence value;*** a property, functionality, attribute or characteristic that an expert witness can use as evidence (usually in court) of fraud having been committed.

***forensic evidence;*** legal information indicating whether something is true or valid

***forensic feature data;*** information deliberately incorporated into a product or document because it has forensic evidence value.

***fraud;*** wrongful or criminal deception intended to result in financial or personal gain

***fraudulent acts;*** actions that are dishonest, untrue, or unfair, and intended to deceive people, e.g.; theft of end product or critical components; theft of critical (functionality) technical data; theft of critical production know-how or equipment; theft of forensic feature data; posing as a bona fide customer; theft of a raw material; theft and disclosure of confidential and or personal information through deception and misrepresentation.

***fraudulent reproduction;*** unauthorized copying

***fraudulent sources;*** customers who are not who they claim to be

***function;*** the action for which something is suited or designed

## H

***hard drive;*** the primary computer storage device in desktop and laptop computers as well as all servers and mainframes that spins, reads and writes one or more fixed disc platters.

***hard evidence;*** legitimate, tangible proof

## I

***IDS;*** intrusion detection system

***incident;*** a security breach

***incidental loss;*** loss occurring as a minor accompaniment or by chance in connection with something else

***information rich offices;*** offices that contain numerous types of information that has been classified as being of strategic value to criminals.

***infrastructure;*** the underlying foundation or basic framework

***innocent disclosure;*** unintentionally disclosed

***integration;*** the acting of combining something with another part or parts to form a whole, or complete product or service.

***integrator;*** an organization having the know how and other wherewithal to combine/assemble a complete end product that completely satisfies the end users requirements.

***internal operations;*** the framework in place within a company that forms the basis of everyday functions

***internal theft****;* stealing that occurs by employees of a company (also known as employee theft)

***intrinsic functional security value****;* the potential that exists in a product to enable fraud to be detected, deterred and controlled. That potential is realized only if the product is properly protected by implementation of security assurance measures.

***intrusion detection systems****;* detection of break-ins or break-in attempts either manually via software expert systems that operate on logs or other information available on the network

***intrusion****;* illegal or unauthorized access to critical information or data

***investment****;* the amount of money spent in exchange for something

***isolate****;* to set apart or cut off from other staff and customers

***IT****;* information technology

## K

***key features of authentication****;* individual, measurable, easily determined properties of validity

## L

***laminates****;* thin, transparent, plastic coatings applied to paper or board to provide protection and give it a glossy finish

***life consequences****;* the potential to reduce the effective operational life of a product.

***limited consequences****;* causes whose effects can be estimated in advance as having small to moderate consequences (not serious consequences)

***logical access****;* re computer security, being able to interact with data through access control procedures such as identification, authentication and authorization

***logistical functions****;* inventory, transport and information systems associated with a product

## M

***manage****;* to control and direct

***market****;* demand for a particular commodity or service

***material control****;* to accurately account, predict the need for supplies and ensure that the right material is in the right place at the right time. In security products processing it includes the requirement to minimize, at all times and stages of processing open access to all special raw materials, special removable tools and computer programs, work in progress and finished products that have security value.

***material handling operations****;* operations throughout production where material is used

***mimic****;* to resemble something in a way that seems like a deliberate copy

***misrepresentation****;* to give an inaccurate or deliberately false account of the nature of oneself, either as an individual or a company

***mitigate****;* to make the result of fraudulent acts less severe

## N

***nature****;* inherent qualities or characteristics

***negligence****;* a civil wrong causing injury or harm to another person or property as the result of doing something or failing to provide a proper or reasonable level of care.

***network documentation****;* the process of providing written details or information about the network

***neutralize;*** to deny access to critical areas or information

***non-disclosure agreement;*** a legal contract between two parties that outlines confidential materials the parties wish to share with one another for certain purposes, but wish to restrict from generalized use

***normal operations;*** regular day-to-day operations within a company

## O

***objective;*** expressing or involving the use of facts without distortion by personal feelings or prejudices

***optical security device;*** a visual security feature that cannot be copied by normal printing and photographic processes and it cannot be peeled off the product as one piece

***origin and batch identity;*** any label, symbol or token that names or identifies the origin of materials and what batch of products it was used for

## P

***perception of risk and reward;*** a way of understanding or interpreting an exposure to danger or loss with a corresponding goal

***personalization;*** custom tailoring information to the individual

***personnel policies and procedures;*** a set of documents that describe an organization's expectations of personnel

***physical intrusion detection;*** see "systems"

***physical intrusion;*** illegal entry upon or appropriation of property of another

***physically insecure;*** an area that does not have a security system in place to control access and egress

***PII; Personally Identifiable Information.*** PII is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.

***presence;*** the existence of something in a particular place

***proactive;*** acting in advance to deal with an expected difficulty

***process of consensus;*** a series of actions toward a particular aim involving general or widespread agreement among all the members of a group

**product**; a tangible item produced by a company that performs a specific function.

***production know-how or equipment;*** specialized knowledge or equipment necessary to create the product

***proportion;*** to the same degree

***protected;*** secured against fraudulent action

***protecting wireless networks;*** the act of making a wireless network immune to eavesdropping an unauthorized intrusion or access.

***public network;*** a network whose access is open to the general public without the need for user ID or password control.

***purchase order;*** a commercial document used to request someone to supply something in return for payment and providing specifications and quantities

## R

***random sample;*** a simple random sample is a subset of individuals (a sample) chosen from a larger set (a population). Each individual is chosen randomly and entirely by chance, such that each individual has the same probability of being chosen at any stage during the sampling process, and each subset of k individuals has the same probability of being chosen for the sample as any other subset of k individuals.

***raw material;*** a basic material from which a product is made

***rectification****;* correction
***remedy****;* to correct
***removable media****;* cartridge and disc-based storage devices which can be used to easily move data between computers with the right readers (e.g. floppy discs, compact discs and flash memory cards)
***removable tools****;* tools designed to be portable.
***retracing events****;* to go back over again each event exactly as it occurred
***risk****;* the probability of loss, injury, disadvantage or destruction of an organization's information resources, existing controls and computer system vulnerabilities. For security products, eight areas of critical security risk have been identified; customer related, information material control, the supply chain, physical intrusion, personnel, disaster recovery and security failure risk. Risk may be expressed as a potential level of damage in dollars and/or other assets.
***risk management requirements****;* compulsory practices towards controlling elements of risk
***risk reduction enhancement****;* an obligatory practice that will increase the security assurance of a product, however, it is not required to obtain certification
***risk reduction infrastructure****;* the underlying foundation or basic framework in place for the purpose of reducing the degree of risk facing a security products producer or consumer

## S

***S.E.I.****;* security end item
***satisfactory****;* fulfills expectations or needs
***scanning system****;* software that searches for known viruses
***secure computing systems****;* a computer system or computer network having very high intrusion resistance.
***securing remote access to the network****;* the act of verifying that a remote request for access to a network is authorized. If not authorized access is then denied.
***security assurance;*** preventing or deterring fraudulent actions and mitigating their effects, if they happen
***security awareness training****;* an educational and skills development course or program that results in persons having a working knowledge of security risks, how to look for them, report them and act upon them.
***security culture****;* beliefs, customs, practices and social behavior of a company's employees that makes security violations socially and morally unacceptable within the group. Those who belong to a security culture also know what behavior compromises security and they are quick to educate and reprimand those people who, out of ignorance, forgetfulness, or personal weakness, partake in insecure behavior.
***security device****;* a piece of equipment designed to serve a special purpose or perform a special function with regard to product security
***security end items;*** products and services that perform security functions and act as a deterrent to prevent fraud
***security functionality;*** how effective a product is as a security product
***security management personnel****;* staff dedicated to creating, implementing and monitoring all of the security requirements of an organization
***security measures****;* actions taken to ensure security

***security patches;*** security software updates meant to fix problems with a computer program i.e. fixing bugs, replacing graphics, improving the usability or performance of a previous version

***security policies and procedures;*** a set of documents that describe an organization's expectations with regard to security

***security product portfolio;*** a collection of security products that are offered for sale by a company

***security product;*** a product that has the potential to enable fraud to be detected, deterred and controlled.

***security substrate;*** a sheet of paper or polymer that acts as a carrier of data and security devices/technologies. The carrier is normally differentiated from common paper and polymer sheet by virtue of having security materials and devices build into to the substrate.

***security technology barrier;*** a technique that significantly increases the difficulty of committing and hiding acts of fraud related to document and product counterfeiting and falsification.

***security technology;*** knowledge of techniques that have the potential to enable fraud to be detected, deterred and controlled.

***security value;*** the value of a security product that is comprised of the combination of the security functionality of the product, it's cost and the degree to which the maker protects it from all forms of fraudulent acts.

***self-assessment of compliance;*** assessment of oneself or one's performance in relation to the NASPO Security Assurance Standards for a particular level of certification

***service;*** useful labor that does not produce a tangible commodity, often involves imparting specialized information or knowledge

***shared risk management;*** equal responsibility between the buyer and the producer to ensure that risks are covered adequately by both sides of the partnership

***single point contact;*** one person

***SNMP;*** Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

***special inks;*** inks having special properties that have been specially formulated for security applications. Normally, such inks are not commercially available.

***specialized security carriers;*** companies that specialize in the distribution of high value and security sensitive shipments

***specifications;*** a detailed description of the necessary standards to be met in order to achieve various levels of certification

***SSID;*** A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN). This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.

***standard use;*** a practice in place throughout a company

***strategic information;*** information that is important or essential to an intended objective

***strategic value;*** the worth of something in terms of its usefulness in executing a plan of action or achieving a goal

***strong authentication;*** the process of establishing the legitimacy of a user before allowing access to requested information. During the process, the user enters a name *or account number (identification) and an alpha numeric password (authentication)*

***sub-contracted work or processing****;* a contract that assigns (contracts out) part of the performance of producing a security product to a third party (the subcontractor)

***subvert****;* to pervert or corrupt for the purposes of undermining the effectiveness of or destroying a security product

***sufficient to warrant****;* meets the qualifying criteria

***supply chain****;* the large and widely distributed group of individuals and/or companies *involved in producing, handling and/or distributing a specific product.*

***syndicate****;* a group of people who combine to carry out a business, enterprise or some other common purpose

***system logs****;* a detailed record of system activity

***enabled****;* to be put into action

***system of control and accountability****;* a process whereby a company is able to track materials and personnel as products are being produced and identify those areas within the process that have failed and provide procedures to remedy those failures

***system security****;* security of the complete computer system within an organization including all CPUs, memory and related electronics, peripheral devices and operating system

***systematic manner****;* carried on using step-by-step procedures

***systems****;* security systems designed to control access into buildings or computers and that detect unauthorized physical intrusion into buildings and secure areas and unauthorized intrusion into computer systems.

## T

***taggants****;* any of various substances, such as microscopic pieces of multilayered colored plastic, added to a product to indicate its source of manufacture

***tailor the criteria****;* to provide the best standard

***tamper evident devices****;* tools specially designed to make it easy to see whether they have been altered

***tamper resistance****;* a property of a document or device that significantly increases both the difficulty of tampering, the difficulty of concealing it and the probability that it will detected.

***technical data****;* highly specialized information that is crucial to the functionality of the product

***technique****;* a way of carrying out a particular task

***terminate****;* to end employment with the company

***termination policies****;* a set of documents outlining personnel practices that will result in *an employee being fired*

***terrorist enabling****;* be of assistance to terrorist activities

***test and promotional samples****;* a product of limited function that is representative of the complete product

***third party custody****;* possession of a product by a company other than the sender or receiver

***time history record****;* an account, in permanent form, of activities undertaken, sorted according to the time of occurrence

***track and trace function****;* the complement to inventory control systems, supply chain management systems, and all those applications that tell people where things should be, where things should go; it allows people to locate where things actually are, where they have been, and (sometimes) where things will be. As opposed to control systems, Track and Trace is the recording of reality.

***transition****;* to pass from one class of certification to a higher class
***transmissions****;* information communicated via radio waves, satellite or wire (i.e. fax, e-mail)

## U

***unauthorized access****;* without permission to retrieve data or use computer equipment that contains sensitive data
***unauthorized verbal communication****;* verbal transfer (disclosure) of security classified information without having obtained prior approval and authorization for the disclosure to be made. Such disclosure is considered to be a breach of security
***unintended disclosure****;* accidentally making secret information known
***unsecured transportation****;* products distributed without a system in place to manage security risks while in transit
***upstream supply chain****;* the individuals and/or companies closer to the security product producer in a supply chain than the final end user

## V

***verifiable controls and procedures****;* systems and operations in place that can be proven as being accurate
***verification****;* to confirm through an auditing process that something is true, accurate, or justified
***verifying delivery****;* ensuring the practice of
***vertical integration****;* when a company expands its business into areas that are at different points of the same production path
***VPN****;* virtual private network
***vulnerabilities****;* areas of exposure to fraudulent activities
***vulnerable****;* susceptible to fraudulent activities

## W

***waste having security value****;* waste material left over from product manufacturing or processing that has security value
***WiFi****;* short for wireless fidelity and is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.
***WEP****;* Wired Equivalent Privacy (WEP) is part of the IEEE 802.11 standard (ratified in September 1999), and is a scheme used to secure wireless networks (WiFi). Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping; WEP was designed to provide comparable confidentiality to a traditional wired network, hence the name. However, several serious weaknesses were identified by cryptanalysts, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the inherent weaknesses, WEP provides a bare minimal level of security that can deter casual snooping.
***WPA****;* Wi-Fi Protected Access (WPA) is a system to secure wireless (Wi-Fi) networks, created to patch the security of the previous system, WEP (Wired Equivalent Privacy).

(Back to Table of Contents )