Transports Canada
Transport Canada
TP 14671
(03/2007)

NOTIONS ÉLÉMENTAIRES DE SÛRETÉ

GUIDE DE RÉFÉRENCE

LA SÛRETÉ MARITIME
TRAVAILLER ENSEMBLE

TC-1002420

Canada

Veuillez acheminer vos commentaires, vos commandes ou vos questions à :

Transports Canada
Sûreté Maritime
112, rue Kent
Place de Ville Tour B, 14e étage
Ottawa (Ontario) K1A 0N5
Courriel : SureteMaritime@tc.gc.ca

TP 14671
(03/2007)

CONTENU

Authorisé / Non authorsé

L'autorisation est fondée sur la décision de la direction de laisser certaines choses arriver, partant du principe que laisser ces choses arriver représente un niveau de risque acceptable. En même temps, l'autorisation appropriée doit être conforme aux obligations juridiques, réglementaires et autres que doit respecter l'organisation.

En ce qui concerne le rendement, pour qu'une tâche soit effectuée ou se poursuive, tout n'a pas à être autorisé explicitement.

Sûreté matérielle

La *sûreté matérielle* compte quatre éléments interdépendants :

1. Des mesures de **prévention** des activités non autorisées;
2. La **détection** des activités non autorisées;
3. Une **intervention** pour stopper une activité non autorisée;
4. La capacité de **rétablissement** suite à une activité non autorisée qui permet de reprendre les opérations normales à un niveau aussi élevé que possible.

On l'appelle : **Prévention, Détection, Intervention et Rétablissement** (PDIR).

Prévention : Couches de protection matérielles, procédurales ou psychologiques servant à décourager ou à retarder une activité non autorisée.

Détection : Le moyen par lequel une violation des mesures de prévention peut être décelée et rapportée, afin de pouvoir déclencher l'intervention appropriée.

Intervention : The procedures and activities used to stop unauthorized activity from the point of notification to the point that the unauthorized activity has been halted.

Rétablissement : La capacité de l'organisation de mesurer l'étendue du dommage causé par l'activité non autorisée, de prendre des mesures pour empêcher que d'autres dommages ne surviennent et de reprendre ses opérations normales.

Défenses par couche

Le but d'un système de sûreté matérielle est de rendre une infraction aussi difficile à commettre que possible. On y parvient en rendant l'approche de sûreté assez solide et complexe pour que :

- l'attaque soit annulée avant même d'être lancée (l'assaillant décide que l'infraction ne vaut pas le risque qu'il soit arrêté), ou
- l'intrusion prend assez de temps pour permettre à l'équipe d'intervention d'agir avant que l'infraction ne réussisse.

Pour que chaque couche soit efficace, elle doit offrir une prévention adéquate en tant que *mesure autonome*, en plus d'interagir avec les autres moyens de défense en place. Les couches ne peuvent être sujettes à la même vulnérabilité.

Le temps est l'élément essentiel et les couches – matérielles ou psychologiques – fournissent le temps nécessaire pour une intervention appropriée.

Barrières matérielles

Les barrières matérielles peuvent être naturelles ou artificielles. Les éléments essentiels de barrières matérielles doivent servir à :

- Réduire le nombre de menaces potentielles, accidentelles ou non intentionnelles (comme le vagabondage);
- Créer un délai suffisant qui permettra l'application de mesures de soutien ou d'intervention (p. ex. le temps d'enjamber une clôture);
- Établir les conditions grâce auxquelles des actions peuvent être déclarées suspectes (p. ex. pourquoi quelqu'un enjamberait-il la clôture?).

La présence de personnel ou le déroulement d'une activité peut servir de barrière matérielle ou même psychologique.

Barrières psychologiques

Les barrières psychologiques servent aussi à démontrer à l'assaillant potentiel que :

- La probabilité d'être arrêté ou identifié est plus grande;
- La cible semble mieux protégée qu'elle ne pourrait l'être en réalité.

De plus, étant donné qu'aucune barrière unique ne peut faire plus que retarder un adversaire déterminé, on doit disposer d'une intervention qui pourra offrir l'aide immédiate nécessaire.

Bien que très utiles dans certaines circonstances, les barrières psychologiques ne doivent servir que de couche défensive de soutien.

Surveillance des espaces

La surveillance des espaces intérieurs implique qu'on indique clairement qu'on exerce le contrôle de ces espaces. En conséquence, les responsables de la sûreté doivent être en mesure de les surveiller à l'aide de moyens appropriés permettant de détecter les activités non autorisées.

La surveillance des espaces répond à la nécessité d'être conscient, à la fois du climat de menace et de ce qui se déroule dans les espaces qui sont contrôlés.

Zones publiques

Les zones d'accès illimité au public sont appelées *zones publiques*. On doit surveiller ces zones pour détecter des activités suspectes.

Zones contrôlées

Les zones contrôlées requièrent un niveau de sécurité plus élevé, où deux critères doivent être respectés. Les personnes et/ou les objets doivent avoir :

1. **L'autorisation** de se trouver dans la zone contrôlée (décision de la direction);
2. **Le droit** de se trouver dans la zone contrôlée (p. ex. pour le travail).

Une fois la confirmation des deux critères établie, on peut autoriser l'accès.

Zones réglementées (ZR)

Les zones r*églementées* exigent le plus haut niveau de contrôle d'accès. Concernant l'accès à une zone réglementée, les personnes et/ou les objets doivent avoir :

1. **L'autorisation** de se trouver dans la ZR (décision de la direction);
2. **Le droit** de se trouver dans la ZR (p. ex. pour le travail); et
3. **Le besoin** de se trouver dans la ZR (exigence spécifique de s'y trouver à ce *moment-là*).

Une fois la confirmation des trois critères établie, on peut autoriser l'accès à la ZR.

Éclairage

La lumière favorise l'utilisation légitime de l'espace, améliore la surveillance naturelle et décourage l'activité criminelle. Il y a cinq principaux points à considérer au sujet de *l'éclairage* :

1. L'uniformité de la lumière;
2. Éviter la création d'endroits de fort éclairage et d'ombres;
3. Les zones ou les activités critiques doivent être illuminées plus intensément;
4. L'interaction avec d'autres systèmes de sûreté et l'impact sur ceux-ci (CCTV);
5. Penser à la sécurité lorsqu'on risque de créer des angles morts.

Un éclairage adéquat peut ajouter au système de sûreté matérielle une couche de dissuasion psychologique efficace.

Systèmes d'alarme

Les systèmes d'alarme détectent un changement dans l'environnement, puis activent un certain type de signal indiquant que l'environnement a effectivement changé. Il existe plusieurs sortes de systèmes d'alarme.

Les systèmes actifs émettent un signal qui, s'il est interrompu ou modifié, déclenche l'alarme. Les systèmes passifs « surveillent » simplement l'environnement et s'activent si les paramètres d'un environnement donné cessent de correspondre à la norme.

Les systèmes d'alarme peuvent produire un signal perceptible (feux clignotants, sirènes, etc.). On les considère souvent comme une mesure de prévention de secours. Lorsqu'on veut capturer un intrus, on peut employer une système d'alarme imperceptible (comme un avertisseur dans un poste de garde).

Dans tous les cas, le système d'alarme doit être associé à un certain type d'intervention et fonctionner conformément aux restrictions matérielles et légales (comme par exemple les règlements sur le bruit) en vigueur dans l'environnement où il se trouve.

Vidéosurveillance

En considérant la technologie de la caméra, on doit tenir compte de l'environnement (personnes, animaux, météo, etc.), des vibrations, ainsi que des restrictions technologiques (notamment la façon dont elle réagit à la lumière), des restrictions légales et réglementaires (les caméras factices exposent l'utilisateur à un degré de responsabilité légale car elles offrent une fausse impression de sûreté.)

La vidéosurveillance peut aussi s'avérer un outil précieux, car elle peut enregistrer les activités et servir aux enquêtes. Il faut veiller à ce que l'information enregistrée soit extraite et conservée de façon sécuritaire, à défaut de quoi, cette information pourrait être rendue inutilisable en contexte juridique.

Par ailleurs, la vidéosurveillance peut être utile pour tirer des leçons.

Patrouilles de sûreté

Les *patrouilles* de sûreté doivent être effectuées régulièrement. Leur fréquence et leur itinéraire doivent être variés afin de ne pas devenir routiniers et analysables. On doit implanter un système d'enregistrement pour voir à ce que toutes les zones à patrouiller soient visitées et indiquer à quelle fréquence elles ont fait l'objet d'une patrouille.

Tout le personnel effectuant des patrouilles de sûreté doit être formé à reconnaître les personnes.

Communications

De bonnes communications sont vitales à l'approche de la sûreté globale. Un *système de communication* efficace permettra au personnel de sûreté en place :

- d'avertir le personnel d'intervention d'une infraction à la sûreté;
- de coordonner l'intervention lors des incidents;
- de transmettre l'information à des organismes extérieurs (au besoin).

Tous les systèmes de communication doivent inclure un système de réserve pouvant fonctionner en tout temps. Les systèmes de communication, y compris les systèmes redondants, doivent être testés régulièrement et les résultats doivent être consignés.

Systèmes et réseaux informatiques

Les ordinateurs et les autres équipements inclus dans un système GI/TI peuvent être installés et fonctionner partout sur le navire ou dans l'installation. En considérant ces systèmes, l'agent de sûreté devrait évaluer la confidentialité des renseignements, l'intégrité des données et la disponibilité du système. Il doit aussi savoir comment utiliser les systèmes et s'assurer que la direction ait clairement communiqué ces instructions d'opération aux utilisateurs de ces systèmes.

Une option consiste à exercer un contrôle central du niveau des permissions aux utilisateurs afin que les personnes puissent accéder à ce dont elles ont besoin, mais pas à tous les systèmes.

Une autre pratique exemplaire consiste à utiliser des mots de passe (y compris le temps de sortie et l'économiseur d'écran exigeant un mot de passe), des coupe-feu, des systèmes de sauvegarde automatique, une alimentation sans coupure et des listes de contrôle. Ces mesures de prévention peuvent procurer des avantages importants quand il s'agit de maintenir le bon fonctionnement des systèmes critiques.

Contrôle d'accès (généralités)

En ce qui touche le contrôle d'accès (personnes et véhicules), l'organisation doit être en mesure de discerner ce qui est autorisé de ce qui ne l'est pas. Toutes les personnes, tous les véhicules et le matériel pénétrant dans l'installation ou le bâtiment doivent d'une manière ou d'une autre passer ce contrôle avant d'y avoir accès. Il doit aussi exister une méthode, comme des rapports hiérarchiques, permettant de clarifier la situation pour déterminer si l'accès doit être accordé.

Dans l'installation ou le bâtiment, il faut être en mesure de déterminer si une infraction s'est passée au point de contrôle et disposer de procédures d'avertissement et d'intervention en cas d'accès non autorisé. De plus, si elle croit qu'il y a eu accès non autorisé, l'organisation doit être capable de prendre des mesures pour déterminer la gravité de tout dommage ou incident de sûreté.

Vehicules

Le contrôle d'accès vise tous les aspects, y compris les conducteurs et les marchandises transportées.

Il y a plusieurs points à considérer concernant l'accès des véhicules, dont les suivants :

- La personne qui a demandé le véhicule est-elle autorisée à lui donner accès?
- Le véhicule arrive-t-il selon l'horaire préalablement établi?
- La présence du véhicule est-elle logique, étant donné sa fonction? (par exemple, on n'attendrait pas un camion à ordures pour un contrat de traiteur)

En tout temps, les documents appropriés (feuille de route, etc.) doivent être présentés, et les détails de l'autorisation ou du refus doivent être consignés.

Sûreté ferroviaire

Les voies ferrées représentent une autre possibilité d'accès à l'installation qui doit être contrôlée, comme toutes autres formes de trafic.

Les wagons laissés sans protection et sans surveillance pourraient donner l'occasion d'y cacher des matières dangereuses. Les zones de transit ferroviaire doivent être déclarées « interdites au personnel non autorisé » et surveillées par des patrouilles afin qu'on se dote d'une capacité adéquate de prévention, de *détection et d'intervention*.

Sûreté des zones riveraines

Pour assurer la mise en place d'une bonne sûreté des *zones riveraines*, il faut travailler en coordination avec des organismes extérieurs pour que ces zones soient patrouillées de façon régulière.

Étant donné la nature de la sûreté des *zones riveraines*, les barrières de prévention sont inappropriées (du point de vue de la sécurité), coûtent très cher et ne sont pas pratiques pour la plupart des applications. Il faut donc s'en remettre à des méthodes de surveillance et de détection accrues afin de réduire l'exposition aux risques créée par l'absence de barrières.

Les procédures d'intervention en cas d'incident de sûreté dans une zone riveraine doivent être détaillées, coordonnées avec d'autres organismes et connues de tous les employés.

Contrôle des clés

Une clé peut être un *objet*, un *jeton* ou un *mot de passe* utilisé pour déverrouiller un verrou, un système ou un autre mécanisme servant à contrôler l'accès à une zone, un bien ou un renseignement spécifique.

L'attribution de clés doit toujours être contrôlée. La personne qui a besoin d'une clé doit présenter une autorisation de la direction lorsqu'elle en fait la demande et avoir été clairement informée sur leur contrôle et leur usage approprié.

Les clés perdues, reproduites sans autorisation ou volées constituent une faiblesse dont on peut facilement profiter si elles ne sont pas signalées. Des procédures doivent prévoir la détection et l'enregistrement des clés manquantes, ainsi que la récupération des clés des employés à leur départ. Suite à la perte d'une clé, les systèmes de contrôle des clés doivent aussi inclure la possibilité de rétablir l'intégrité des mesures de prévention que cette clé contrôle habituellement. Les clés non attribuées ou les passe-partout doivent être numérotés et conservés dans un coffre de sûreté.

Identification

Un outil d'*identification* doit principalement :

- Identifier qui est autorisé et qui ne l'est pas;
- Doit être unique à l'environnement et aisément identifiable;
- Ne doit pas pouvoir être altéré ou modifié

Les contrôles doivent être strictement maintenus et inclure la vérification régulière des pièces d'identité annulées, perdues ou volées.

Les véhicules dont l'accès est autorisé doivent porter une marque d'identification à cet effet.

Les marques d'identification des véhicules doivent indiquer qu'elles appartiennent à l'autorité compétente et doivent lui être retournées sur demande.

Formation et sensibilisation

Les employés, ayant ou non des responsabilités en matière de sûreté, doivent posséder des connaissances relatives au *Règlement sur la sûreté du transport maritime*. Grâce à ce genre de formation et de sensibilisation, on veille à ce que les employés connaissent leurs responsabilités relatives à la sûreté, les dispositions du plan de sûreté et les procédures d'intervention en cas d'incident de sûreté. En ce qui concerne les employés n'ayant pas de responsabilité de sûreté, une orientation en matière de sûreté permet de leur faire connaître les différents niveaux de sûreté et reconnaître les objets ou comportements suspects, ainsi que les techniques qui pourraient être utilisées pour éviter les mesures de sûreté ou les faire échouer.

Il faut donner une formation d'appoint une fois par année et suite à tout incident de sûreté majeur, afin que les employés détiennent les connaissances les plus récentes possibles sur les enjeux de sûreté, les procédures et toute modification apportée.

Ces séances peuvent aussi être coordonnées avec des exposés sur les mesures de sécurité, de manière à offrir une approche plus globale aux visiteurs.

Entraînements et exercices

Pour bien implanter l'une ou l'autre des mesures du plan de sûreté, il faut tenir des entraînements et des exercices. Ils serviront non seulement à vérifier si les employés connaissent et observent les procédures et les responsabilités durant un incident, mais aussi à voir à ce que toutes les facettes de l'évaluation de la sûreté aient été couvertes.

À la fin de chaque entraînement ou exercice, il faut faire le bilan avec tous les participants pour discuter de ce qui a bien fonctionné et de ce qui peut être amélioré. Les leçons tirées doivent être consignées, et toute lacune relevée devra être réparée (de l'évaluation de la sûreté jusqu'au plan de sûreté).

Examen des systèmes de sûreté

Les systèmes de sûreté doivent régulièrement faire l'objet d'un examen pour vérifier qu'ils fonctionnent correctement et efficacement. De plus, les systèmes de secours pour chaque couche doivent être examinés et testés afin de s'assurer qu'en cas de panne, ils puissent rapidement prendre la relève pour remédier à la vulnérabilité créée par cette panne.

NOTES

Transport Canada
Transports Canada
TP 14671
(03/2007)

SECURITY FUNDAMENTALS

QUICK REFERENCE GUIDE

MARINE SECURITY
WORKING TOGETHER

TC-1002420

Canada

Please direct your comments, orders and inquiries to:

Transport Canada
Marine Security (ABM)
112 Kent Street
Place de Ville Tower B, 14th Floor
Ottawa, Ontario K1A 0N5
Email: MarineSecurity@tc.gc.ca

TP 14671
(03/2007)

CONTENTS

Authorized / Unauthorized

Authorization is based upon management's decision to allow certain events to happen given that the resulting impact(s) fall within an acceptable level of risk. At the same time, authorization must also comply with legal, regulatory and other obligations that must be met by the organization.

With respect to performance, in order for work to happen and/or continue, not all events, people or objects have to be authorized explicitly.

Physical Security

Physical Security is comprised of four interdependent elements:

1. Measures for the **Prevention** of unauthorized activity;
2. **Detection** of unauthorized activity;
3. A **Response** to stop an unauthorized activity; and
4. The ability to **Recover** from an unauthorized activity that allows for the return to normal operations, to the highest degree possible.

This is known as **Prevention, Detection, Response** and **Recover** (PDRR).

Prevention: The physical, procedural or psychological layers used to deter or delay unauthorized activity.

Detection: The means in which a breach of preventative measures can be identified and reported so that the appropriate response can be initiated.

Response: The procedures and activities used to stop unauthorized activity from the point of notification to the point that the unauthorized activity has been halted.

Recovery: The ability of the organization to determine the extent of injury caused by unauthorized activity, take steps to halt the further spread of damage and return to normal operations.

Layered Defenses

The purpose of a physical security system is to make a successful breach as difficult as possible. This is done by making the security posture adequately strong and complex enough so that an attack is:

- Called off before being started (attacker decides it's not worth the risk of being caught), or
- Delayed long enough for a response to intercept the breach before it becomes successful

In order for layers to be effective, each layer must be able to provide ample prevention as a *stand-alone measure* and, work in conjunction with other defenses in place. Layers cannot be subject to the same vulnerability.

Time is the essential element. Layers, physical or psychological, provide a time delay to initiate a proper response.

Physical Barriers

Physical Barriers can be natural or man made. The essential criteria of a physical barrier are as follows:

- Limit the number of potential, accidental or non-intentional threats (ex. loitering);
- Create a sufficient time delay to allow for supportive or response actions to take place (ex. time to climb a fence); and to
- Provide the conditions by which actions can be declared suspicious (ex. why would anyone climb the fence?)

The presence of personnel or activity can act as a physical and/or psychological barrier.

Psychological Barriers

Psychological barriers are measures that would cause an attacker to perceive:

- The probability of being caught or identified as increased
- The target as being better protected than it may actually be

Because no single barrier can do more than delay a determined adversary, response must provide the necessary back-up protection.

Psychological barriers, while very useful in some circumstances, should be used as a supporting layer of defense.

Monitoring of Spaces

Monitoring involves clearly indicating that control is being exercised. Security must also be able to monitor activity within an area using appropriate means to detect un-authorized activity.

The monitoring of spaces responds to the need to be aware of both the environment and what is occurring within these areas.

Public Areas

Areas in which the public has open unrestricted access. These areas should be monitored for suspicious activity.

Controlled Areas

Controlled Areas require a heightened level of security in which two criteria must be met. People and/or objects must:

1. Be authorized to be in the controlled area (i.e. a management decision),
2. Have the right to be in the controlled area (ex. for work purposes).

Once confirmation of both criteria has been established, access can be granted.

Restricted Areas (RA)

Restricted Areas require the highest level of access control. When looking at access to a restricted area, there are three criteria that must be met. People and/or objects must:

1. Be **authorized** to be in the RA
   (i.e. a management decision),
2. Have a **right** to be in the RA
   (ex. for work purposes),
3. Have a **need** to be in the RA
   (i.e. a specific requirement to be in the RA at that time)

Once confirmation of all three criteria has been established, access to the RA can be granted.

Lighting

Light encourages legitimate use of space, enhances natural surveillance and discourages criminal activity. There are five main areas of consideration for *lighting*:

1. Evenness of the light,
2. Avoidance in creating bright spots and shadows,
3. Targeting critical areas or activities
   (should be illuminated more brightly),
4. Interaction with, and impact on, other security systems
   (ex. CCTV),
5. Safety in regards to the creation of blind spots.

Adequate lighting can provide an effective psychological deterrent layer to the physical security system.

Security Alarms

Security alarms detect a change in the environment and then activate a signal to broadcast the fact that the environment has indeed, changed. There are several different kinds of alarms available.

Active alarms will send out a signal that, if interrupted or changed, triggers the alarm. Passive alarms simply "watch" an environment and are activated only if the environment moves outside of certain set or configured parameters.

Alarms can provide a noticeable signal (ex. flashing lights, sirens, etc.), however these are often back-up prevention measures. Where capture of an attacker is sought, an unnoticeable alarm (such as a buzzer in a control center) may be used.

In all cases, the alarm itself must be tied to some kind of response and take into account the physical and legal restrictions (ex. such as noise bylaws) of the environment in which it operates.

Video Surveillance

When looking at camera technology, care should be taken to consider the environment (ex. people, wildlife, weather, etc), vibration, technological restrictions (particularly how it interacts with lighting) and legal / regulatory restrictions (dummy cameras open the organization to a level of legal liability by providing a false level of security).

Video surveillance can also provide a valuable tool in terms of its ability to record activities which may be useful for investigations. Care should be taken, however, to ensure that information is retrieved and stored securely as failures to do so may render footage unusable in a legal context.

In addition, video surveillance may be used for “lessons learned” activities.

Security Rounds

Security rounds are to be performed on a regular basis. The frequency and routes of rounds should be staggered to avoid routine that could be monitored. A logging system should be implemented to ensure that all areas that are required to be patrolled have been covered - and at what frequency.

All personnel performing security rounds are to be trained in the recognition of suspicious items and persons and the appropriate response procedures.

Communications

Effective communications are essential to the overall security posture. An effective *communications system* will allow security personnel to:

- Notify response personnel of a breach in security;
- Coordinate response to incidents; and
- Communicate to outside agencies (if required)

All communications systems should include back-up mechanisms to ensure operation at all times. Testing communications systems, including the redundant systems, must be performed (and results recorded) on a regular basis.

Networks / Computer Systems

Computers and other equipment included as part of an IM/IT system, may operate throughout the ship / facility. When looking at these systems, the security officer should consider the confidentiality of the information, integrity of data, and availability of the system. In addition, the security officer must have knowledge of the appropriate use of the systems and ensure that these practices are clearly communicated under management's authority.

IM/IT security may be centrally controlled to ensure the level of permissions for users limit a person to have access to what they need, but not to all systems.

Other best practices include ensuring the use of passwords (including session time-outs and the use of screensavers with password prompts), firewalls, back-up systems, uninterrupted power supplies and audit logs. These preventions can offer significant benefits in terms of keeping critical systems operating as required.

Access Control (General)

When looking at Access Control (both of persons and vehicles), the organization must be able to identify what is authorized and what is not. All persons, vehicles or material entering the facility/vessel must undergo this verification before being granted access. There should also be a method to confirm if access should be granted such as a line of communication.

The facility/vessel must also have the means to detect a breach at the control point as well as procedures for reporting and responding to unauthorized access. Where unauthorized access is successful, the organization must take steps to determine the extent of the security incident and any injury incurred.

Vehicles

Access control pertains to all aspects including the driver and cargo.

Verification for vehicle access should take into account the following questions:

- Was the vehicle requested by someone with the authority to grant it access?
- Is the vehicle expected at that time?
- Does the vehicle correspond to its purpose (ex. a garbage truck would not be expected for a catering contract)?

At all times, relevant documentation (ex. waybills) must be presented and details of the entry/refusal recorded.

Rail Security

Rail lines provide another avenue of access onto the facility and must be controlled in the same manner as any other form of traffic.

Unsecured and unmonitored rail cars may provide an opportunity to hide dangerous material. Rail staging areas should be declared as “Off Limits to Unauthorized Personnel” and monitored with patrols to provide adequate *prevention/detection/response* capabilities.

Waterside Security

For facilities, in order to provide adequate *waterside security*, coordination with outside agencies is necessary to ensure that those areas are patrolled regularly.

Due to the nature of waterside security, preventative barriers are inappropriate (from a safety perspective), very expensive and impractical for most applications. This means that increased monitoring and detection methods must be used to reduce the risk exposure created by the lack of barriers.

Response procedures for waterside security incidents must be detailed and coordinated with other agencies and known to all employees.

Key Control

Keys include any *asset, token* or *password* that unlock a lock, system or some other mechanism used to control access to a specific area, asset or information.

Issuing of keys must be controlled at all times. Personnel requiring keys should produce management authorization as part of the request and be briefed regarding their appropriate control and use.

Lost, inappropriately copied or stolen keys provide a weakness that can be easily exploited if unreported. Procedures should be in place to detect and record missing keys and ensure that keys are collected from employees upon departure. Key control systems should also include the means of recovering from the loss of a key. This ensures the integrity of the asset normally controlled by the key. All un-issued or master keys should be kept in a secure storage container and numbered.

Identification

The main criteria for an Identification tool are as follows:

- Identify who is authorized and who is not;
- Must be unique to the environment and be easily identifiable; and
- Must not be susceptible to tampering or modification

Controls should be strictly maintained and include regular audits of cancelled, lost and or stolen identification cards.

Vehicles that are granted authorized access should be given some form of identification marker.

Identification markers should include some indication that it is the property of the issuing authority and must be returned upon request of that authority.

Training and Awareness

Employees (with and without) security responsibilities are required to possess specific knowledge under the Marine Transportation Security Regulations (MTSRs). This type of training and awareness ensures that employees with security responsibilities are educated on their specific responsibilities relating to security, the relevant provisions of the security plan and response procedures to security related incidents. For personnel without security responsibilities, a security orientation provides knowledge on the different security levels, the recognition of suspicious objects and behaviors and the techniques that might be used to circumvent or cause the failure of security measures.

Refresher training is to be held on an annual basis and following any significant security incident. This will ensure that employees are as current as possible on security issues, procedures and any changes that may have occurred.

These sessions might also be coordinated with Safety briefings in order to provide a more holistic approach.

Drills and Exercise

To effectively implement the procedures within the security plan, drills and exercises must be conducted. These will not only verify that procedures and responsibilities are known and followed during an incident, but will also ensure that all areas of the security assessment are addressed.

Following any drill or exercise, an all-participants debriefing should take place to discuss areas of success and areas that require improvement. Lessons learned must be recorded and any deficiencies noted are to be dealt with (beginning at the security assessment and working through the security plan).

Review of Security Systems

Review of security systems must be conducted on a regular basis to ensure that each component is functioning properly and effectively. Back-up systems for each layer must also be reviewed and tested to ensure that it could be quickly activated to mitigate the vulnerability created by a failure.

NOTES