Site and Supply Chain Security Guidance

PACIA

This guidance does not attempt to provide an inclusive list of recommended security measures. Further, the guidance in this document is not intended as a substitute for requirements under applicable Federal, state or local security related legislation.

Site and Supply Chain Security Guidance

Contents

Section 1: Introduction

1.1 Security a fundamental part of good business

Security is now a fundamental part of good business management and should be viewed as another facet of risk management. Security should be part of an organisation's culture, and integrated into its philosophy, practices and plans.

Today's heightened concerns about terrorism reinforces the importance of security's place in our business operations, and that we must continually review security measures and respond to varying circumstances and threats.

Industry, management, employees and contractors through their daily actions need to actively participate in securing the industry. Everyone is responsible for security.

It is vital that industry takes a holistic approach to security. PACIA members need to ensure that they maintain a focussed relationship along the whole supply chain.

All links in the supply chain must be considered including third party manufacturing, transport, warehousing, customer carriers and customer locations. Product stewardship principles mean that individual companies should consider how they influence their retail chain.

1.2 Sustainability Leadership Framework

The PACIA Sustainability Framework identifies the priority areas for the plastic and chemical industry to respond to, adapt and transform to remain competitive and profitable in the future.

Security is one of the eleven priority areas identified for action in order to position the industry for the future. The chemical industry must continue to respond to the challenge of increased security measures. Operating and delivering secure sites and products is essential to maintain continued operations.

Incorporating security into your business will help you to continue in business whilst protecting your people and operations, and maintain viability and profitability whilst addressing the community need for security.

1.3 National Counter-Terrorism Alert System

The National Counter-Terrorism Alert System is a range of four levels that communicate an assessed risk of terrorism to Australia. The Alert System guides national preparation and planning. It also dictates levels of precaution and vigilance to minimise the risk of a terrorist incident occurring.

The National Counter-Terrorism Alert System is a flexible, tiered system that may be applied where necessary:

- nationally;
- across impacted States or Territories;
- industry/business sectors;
- or geographic locations.

The flexible system recognising geographic areas or industry sectors was introduced in October 2008. Prior to then an alert level change could only be applied to the entire nation.

Alert levels may also set at the state level to provide more specific and targeted information.

Information about this can be obtained from
http://www.nationalsecurity.gov.au/agd/WWW/NationalSecurity.nsf/Page/Information_for_Individuals_National_Security_Alert_System_National_Counter-Terrorism_Alert_System

While the Alert System may not directly affect your day to day life or business, it is important that you are aware that these arrangements exist. As alert levels can change quickly, business should regularly keep informed of the current situation.

1.4 Consultation and partnerships

Information, Community Right to Know (CRTK) and Security

Openness and transparency towards stakeholders are inherent in the modern business practice and part of the Responsible Care system. However, this must also be considered from a security perspective. Requests for information under the Responsible Care® CRTK program must be balanced against disclosure from the security viewpoint, taking into account individual circumstances and the level of threat.

The level of threat can change very quickly. It must be ensured that the sharing of information does not negate security measures that are a part of a heightened security level plan. Any information that identifies areas of security vulnerability must not be disclosed.

Links with Relevant Agencies

A company security policy must be developed in consultation with employees, local community (if applicable), local police, security agencies or other law enforcement agencies, and companies within the supply chain.

Consideration should be given to establishing partnerships or enhancing relationships with local, state, and federal security and other public safety agencies such as Police. Brief them on your security measures and determine what assistance they may need from you. Through such a network, you may learn more easily of looming threats, dangerous trends, and successful and unsuccessful security measures.

Public safety agencies such as law enforcement agencies and local police should be made aware of developments and any changes that are might affect the security of a site.

Partnerships with security services are also be encouraged. If security is breached it is security services that can provide you rapid support to secure you site and local, state and possibly federal police departments that will be engaged with the company to investigate the incident.

Critical Infrastructure Protection Units

Developing a relationship with the Critical Infrastructure Protection units within each state can be useful in understanding on going threats.

The Critical Infrastructure Protection Branch of the Attorney-General's Department is responsible for the development and coordination of Australian Government policy and international cooperation relating to critical infrastructure protection. A range of inter-governmental and business government consultative mechanisms have also been established, to assist in the development and coordination of national security policy.

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) enables the owners and operators of critical infrastructure to share, on a national level, information on important issues such as business continuity, consequence management, and threats and vulnerabilities.

The TISN is a forum where the owners and operators of critical infrastructure work together, sharing information on the security issues that affect them. It provides a safe environment where industry and government can share vital information on critical infrastructure protection and organisational resilience.

Similar networks are established in each State and Territory.

ASIO Business Liaison Unit (BLU

The ASIO Business Liaison Unit (BLU) has been established to provide an interface between Australian Business and the Australian intelligence community. The BLU aims to ensure that owners and operators of critical infrastructure and other relevant members of the Australian business community can assess timely ASIO information on matters affecting the security of assets and staff for which they are responsible. Businesses can use this information to inform their risk management processes. In addition to facilitating the direct dissemination of ASIO information to Australian businesses, the BLU provides businesses with a point of contact for the Australian intelligence community and notification of upcoming security presentations and events.

The ASIO Business Liaison Unit produces reports which can be used for information when carrying out security risk assessments. Companies handling chemicals of security concern would benefit from membership. Access to the BLU information is through a secure website. Application for access is through their website (http://blu.asio.gov.au/home), and is encouraged.

Chemical Security Website

In October 2008, COAG agreed to the establishment of a Chemical Security Management Framework. The Attorney-General's Department is responsible for the coordination of the national implementation of the Framework. The Framework is set out in the Intergovernment *Agreement on Australia's National Arrangements for the Management of Security Risks Associated with Chemicals*.

The Chemical Security Website provides information on the framework established the development and implementation of measures to enhance the security of chemicals, the community awareness campaign and the mechanisms established to address this issue.

Further information on the identified chemicals of concern and the Framework can be found in **Appendix A**.

It is essential to:

- **Develop or integrate a security policy into the business**
- **Undertake security hazard and risk assessments**
- **Assess site security needs**
- **Undertake awareness raising and security training**

Supply Chain

Establishing a security focussed relationship along the supply chain is strongly encouraged. Development of security plans in isolation from other parts of the chain can create weaknesses that may not be obvious to the individual, but through discussion these gaps can be identified and actions taken to close them.

Further information on establishing this relation can be found in **Section 4.2**

Section 2 Security Risk Management

Security risk management is a fundamental part of good business management. It should be part of an organisation's culture, and integrated into its philosophy.

Risk management should follow the process defined in ISO 31000 Risk Management – Principles and Guidelines. Various risk analysis models could be used including those within Standards Australia Security Risk Management Handbook (HB167:2006).

2.1 Make someone responsible for security in the company

Security management responsibility generally should be assigned to one person. Their role could consist of:

- reviewing and ensuring compliance with security related legislation;
- establish relationships with security, police and public safety agencies and surrounding communities (where applicable) to address security concerns
- promoting the company security policy
- developing and manage incident reporting systems,
- assisting in raising employees' security awareness,
- referring security breaches for investigation,
- coordinating emergency response and
- periodic assessment of the company's security program.

2.2 Include security in employee and contactor training

It is vital that all relevant employees and contractors receive induction and ongoing training in physical security and the security policies of the organisation.

Employees and contractors see much that occurs in and around a chemical facility and are in a good position to notice when something or someone does not seem quite right. Training on suspicious behaviour and activity, and awareness measures can transform employees and contractors into a natural surveillance system.

2.3 Ensure suspicious incidents and security breaches are reported and investigated

All suspicious incidents and security breaches (of company policies) must be investigated. By keeping detailed records of suspicious incidents and security breaches, you may be able to spot trends and piece together facts that lead to successful investigations.

The following are some types of security incidents that would warrant investigation:

- Doors not secured, holes in fence lines, indication of illegal entry
- Unauthorised entry by personnel into restricted areas of the facility
- Signs of vehicles in restricted areas along pipelines, fence lines, electrical substations, or remote plant security gates

- Individual(s) asking for technical information about the facility that could be used by an adversary to cause harm
- Major unexplained process upsets
- Unexplained loss of containment of hazardous material
- Unexplained loss of raw material or product
- Major cyber attack against internal process control systems

2.4 Inventory Management

Any loss or suspected theft of chemicals, or suspicious or suspected illegal activity should immediately be reported to the police.

Knowledge of your inventory and the quantity of chemicals stored at any one time is vital. Keep all records of materials received and dispatched. Be aware of specific chemicals that may be diverted into criminal or terrorist activities including the development of chemical weapons, illicit drugs or explosives. Such chemicals will require a specific focus in your risk assessment. (See Appendix A for further assistance.)

2.5 Employment Screening

Identity checking of new employees and contractors is an important component of a company's risk management strategy. The necessity and extent of any employment screening should be based on the risks that the position exposes the organisation to. Accordingly, not all positions will necessarily require employment screening.

A useful resource to assist is the Australian Standard AS4811-2006 – Australian Standard – Employment Screening and HB323-2007 – Employment Screening Handbook

Section 3 Risk assessment

A security risk assessment should be conducted to take stock of the assets that need to be protected, the threats that may be posed against those assets, and the likelihood and consequences of attacks against those assets. Then, put appropriate controls in place to deal with the risks – see **Section 4 Risk Management**.

The risk assessment process is well understood by most companies but in summary a security risk assessment includes:

- **Identifying the assets that need to be protected;**

  Assets are broadly defined as people, information, and property.

- **Assess the threats, vulnerabilities, and consequences**

  Once assets have been identified, you should consider which assets might be vulnerable. This procedure helps identify and prioritise likely targets and saves companies from expending resources where the likelihood of a security breach is remote.

ISO 31000 Risk Management – Principles and Guidelines and HB 167:2006 are useful resources and outline a broad framework and core processes that should be included in a security risk management process.

The risk assessment is then used to identify and close gaps in security arrangements, on-site emergency/crisis plans, business continuity plans, and recovery plans, and to implement appropriate risk management controls.

Section 4 Risk Management

There is no one-size-fits-all approach to risk management, nor is there a one-size-fits-all approach to security. The risk assessment process will determine the risk management practices adopted.

The treatment of security threats will need to be specific to your site and include a combination of protective measures. One model that is well suited to chemical facilities known as the D^3R^2 is outlined in **Appendix B**

Develop a Response and Crisis Management Plan

In the chemical industry, **emergency response** and crisis management functions are to a large extent covered by government regulation. Proper crisis management may prevent an intrusion or attack from becoming a major incident.

Business continuity and recovery planning should be considered while developing emergency response and crisis management plans.

It is important that a **security response plan**, as well as an emergency response plan is created. A security incident may have created an emergency for the organisation involved but the security response will likely have differing actions to the response for a safety related incident.

Security plans should include:

- The security capacity to be escalated quickly if there is reliable intelligence that the security level for a company has been escalated.

  For example: at a medium (current) level of security threat the organisation is carrying out random vehicle searches once a week, at a high security level, random vehicle searches daily and at extreme security level every vehicle entering or leaving is searched.

- Regular inspection of physical aspects and regular review of personal security trends.

  These should include patrols and inspections on a regular basis of fences, buildings, the operations of automatic gates and area lighting.

- Capacity to quickly respond to a breach of security, including repair to physical security protection or restoration of security system.

  Systems need to be in place to ensure that any breach of security fences, correct operation of gates or in some cases lighting can be quickly reported and secured (possibly temporarily), with capacity to implement corrective actions within a time line which may vary based on the threat level.

- Specification of security locks to be used and the control of keys.

  Locks used for security purpose should be to a dedicated pattern for each organisation with a documented procedure for control of issuing and return of keys

- Identity checking of new employees and contractors coming on to site. Reference should be made to HB 323: 2007 Employment Screening Handbook.

Conduct periodic security reviews

You should review your company security measures periodically, as well as whenever facilities or other conditions change significantly. Include security in any self assessment or audit of operational procedures. It may also be useful to do the following at appropriate intervals:

- Update risk assessments and site surveys.
- Review the level of employees' and contractors' compliance with security procedures.
- Consider whether those procedures need modification.
- Ensure appropriate ongoing testing and maintenance of security systems (such as access control, intrusion detection, and video surveillance).
- Ensure that personnel security is included in any review.

4.1 Site Security

The level of security at your facilities should be commensurate with the level of risk determined in the risk assessment process. Make the security visible to your employees and the community.

Be especially careful in admitting visitors to your facility. Ensure all visitors report to the Reception area first. Know who they are, and verify that they have legitimate reasons for being at your site. Use an ID badge/sign-in system. Visitors should be accompanied at all times while on site.

Elements of site security may include access control, perimeter protection, use of security officers, and other measures. NOTE - Facilities determined to be major hazard facilities (MHFs) may be subject to specific security requirements under MHF or other legislation.

Access Control

The appropriate level of access control varies significantly from facility to facility. It depends on the number of employees, hazards of materials present, level of pedestrian and vehicular traffic into and out of the facility, degree to which facility operations are controversial, attractiveness of the facility as, proximity of the facility to populated areas, and many other factors.

The following are just a few of the measures that you may wish to consider for the purpose of controlling access into, within, and out of a chemical facility:

- Post "No Trespassing" and "Authorised Access Only" signs.
- To the extent feasible, employ natural surveillance by arranging reception, production, and office space so unescorted visitors can be noticed easily.
- Install appropriate locks on exterior and interior doors.
- Keep publicly accessible restroom doors locked and set up a key control system. If there is a combination lock, only office personnel should open the lock for visitors.
- Require visitor sign-in logs and escorts.
- Pay close attention to access control at loading and unloading areas.
- Install appropriate, penetration-resistant doors and security hinges.
- Install secure windows with appropriate locks.

- Institute a system of employee and contractor photo ID badges. Train employees to challenge persons who are not wearing badges.
- Establish a system for determining which cars, trucks, rail cars, marine vessels, and other vehicles may enter the site, through which gates, docks, or other entrances, and under what conditions. Such a system may be part of the pedestrian access control system, relying on key cards carried by vehicle operators, or it may be an independent system relying on staffed security posts.
- Install an electronic access control system that requires the use of key cards at main entrances and on other appropriate doors and that provides an audit trail of ingress and egress.
- Install a closed-circuit television system to monitor key areas of the facility.

Perimeter Protection

Controlling the movement of people within a facility is important, but it is far better to stop intruders—whether they are terrorists, saboteurs, vandals, thieves, or protesters—at the edge of a facility's property, long before they reach vital assets and operational areas.

Perimeter protection includes such measures as these, which you can consider and implement as appropriate:

- Fences and exterior walls that make it difficult for intruders to enter the site
- Bollards and trenches that prevent vehicles from driving into the site at points other than official entrances
- Vehicle gates with retractable barriers
- Personnel gates and turnstiles
- Setbacks and clear zones that eliminate hiding places near the site's perimeter, making it difficult for intruders to approach the site unnoticed
- Lighting that makes it easier for employees and even passers-by to observe and possibly identify intruders
- The installation of CCTV may also be considered.

Security Personnel

If it is deemed appropriate for a site to have security officers, you should consider whether the officers will tour the site or remain at fixed posts; whether they will be contract or in-house officers; and what training and licensing they should receive.

Backup Systems

From a security standpoint as well as a safety and operations standpoint, it may be appropriate for chemical facilities to secure as far as possible such utilities as electricity, communications (telephone and computer), water, sewer, and gas. Crucial communications equipment and utility areas can be protected with locks and with alarms that ring to a location that is staffed around the clock. Wiring can be protected by being placed in rigid conduit so it cannot easily be cut.

Subject to the risk assessment, key resources such as control centres, computer servers, and telecommunications equipment may warrant a backup power source, eg. a generator.

Other Considerations

At a chemical facility, managers should keep in mind that any physical security hardware must be safe for use in that particular facility. For example, closed-circuit television cameras and access control card readers may need to be specially selected so they are safe and effective in corrosive or flammable areas.

In addition, any site redesigns should be done with security in mind. For example, plants should generally be laid out so that the most vulnerable or important locations are hardest for adversaries to reach.

4.2 Supply Chain Security

It is important that you:

- **Implement supply chain product stewardship measures;**
- **Partner with supply chain partners to share safety and security awareness, expertise and resources;**
- **If practical develop product based solutions, such as odourants, colourants and managements systems,**

A risk management approach should be applied to all aspects of the supply chain. Identify the assets to be protected, assess the threat, vulnerability and consequences of a security breach, and implement appropriate controls to handle the risk. Consideration needs to be given to all the links in the supply chain including third party manufacturing, transport, warehousing, customer carriers and customer locations.

Your customers

Product Stewardship requires effective management of the risks associated with products through the supply chain. Particular emphasis is placed on active dialogue with customers and other direct product recipients.

Verify that all customers are legitimate and have legitimate uses for the product(s) you are supplying. Security can involve close monitoring of all sales of products, particularly products containing chemicals whose toxicity, physical properties and availability makes them potentially suitable for terrorist use. Dialogue with purchasers can include, if appropriate, discussing security arrangements for the safe storage of such products.

It's better to ask questions, and be particularly wary if:

- **the customer is previously unknown and their identity is unclear**
- **the customer pays cash, even for large orders**
- **the customer is reluctant to explain – use for products, location of premises where products are to be used, or makes an unusual request for excessive confidentiality regarding final destination for product**
- **merchandise is collected with purchaser's own vehicle**
- **a customer transaction involves a third party or intermediary – which is unusual to the customer's normal business practice**
- **the customer lacks business acumen and lacks standard business stationary**
- **they are reluctant to supply a written order**
- **the order contains more than one precursor chemical**
- **the purchase does not match a customer's usual business**
- **the order is for a university or well know company where the normal ordering arrangements are used, but delivery is requested to a specific individual**
- **the customer declines an offer of technical assistance when this is a standard part of the transaction**
- **the customer offers unusually favourable terms**

Controls that could be considered are:

- **record keeping,**
- **no cash sales,**
- **where possible, use account customers,**
- **the specific identification of the purchaser,**
- **locked storage,**
- **monitoring of sales, and**
- **the completion of a signed End User Declaration*.**

* Information on End User Declarations can be obtained from the PACIA Code of Practice for Supply Diversion into Illicit Drug Manufacture.

You should be sure that you are aware of any specific security legislative or other requirements on chemicals for example regulations on security sensitive ammonium nitrate and the Chemicals Weapons Convention.

Transport security

Carefully monitor deliveries and distribution of materials and products to and from your site. Common sense applies:

- Know the carrier – supplying into and distributing out of your facility;

- For deliveries - verify that the delivery is expected, and inspect the delivery vehicle; check the goods are what you are expecting;
- Do not accept unscheduled deliveries. Only known vehicles should be allowed on the premises, and
- Ensure that vehicle access points to the site are controlled in such a way as to prevent "tailgating".

Ensure you comply with all relevant security requirements under Federal and/or State dangerous goods transport legislation.

Maritime security

Maritime Transport Security Legislation

The Maritime Transport Security Act 2003 establishes a regulatory framework that safeguards maritime transport against unlawful interference. In particular, the framework is aimed at protecting ships, ports and port facilities within Australia, and Australian ships operating outside of Australia. The Maritime Transport Security Regulation 2003 complements the Act.

Further information can be obtained from the federal government website – Maritime security: http://www.infrastructure.gov.au/transport/security/maritime/index.aspx

Appendix C provides further information that may be issued to customers to support their endeavours to control chemicals of security concern.

4.3 IT and Information Security

In a chemical facility, protecting information and computer networks means more than safeguarding a company's proprietary information and keeping the business running, as important as those goals are. It also means protecting chemical processes from hazardous disruptions and preventing unwanted chemical releases.

A useful standard is **ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements**

This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organisations or parts thereof.

CERT Australia is Australia's official national computer emergency response team (CERT). CERT Australia works to ensure that all Australians and Australian businesses have access to information

on how to better protect their information technology environment from cyber based threats and vulnerabilities.

CERT Australia's primary responsibility is to work with the private sector in identifying critical infrastructure and systems that are important to Australia's national interest, based on an assessment of risk, and to provide these organisations with information and assistance to help them protect their information and communication technology infrastructure from cyber threats and vulnerabilities. This is also achieved through trusted information exchanges between the Australian Government and Australian businesses on cyber security issues. In working to protect critical infrastructure such as banking, water, energy generation, transportation and telecommunications, CERT Australia plays a part in ensuring those services that all Australians rely on are secure and resilient. Further information can be obtained from their website.

Operations Security

It is vital to protect information that could be useful to criminals, demonstrators, and terrorists who wish to plan attacks on a chemical site or obtain hazardous materials for weapon building. Examples of such information include:

- Process flow diagrams
- Piping and instrument design diagrams
- Formulations
- Client and supplier lists
- Site maps
- Other information that describes the workings of a chemical facility

The risk assessment should also include an IT aspect, examining threats, vulnerabilities, and consequences from this perspective.

Cyber attack includes hacking into the IT system or introducing viruses to:

- corrupt data;
- disable or alter controls; and
- prevent emergency response systems.

A variety of measures for enhancing computer and network security exist, including:

- Employ firewalls, virus protection, encryption, user identification, and message and user authentication to protect both the main computer network and any subsidiary networks, such as access control systems, that are connected to it or to the outside.
- Teach employees to beware of ruses to obtain their computer passwords.
- Require systems administrator to disable all Internet connection software that may be pre-packaged in operating systems.
- Allow the principles of "least access," "need to know," and "separation of functions" to guide the determination of user authorisations, rather than position or precedent.
- Do not post signs indicating the location of the computing facility.

- Equip the computer room with adequate communications capabilities to facilitate prompt reporting of emergencies.
- Allow only authorised personnel to have physical access to central computer rooms. Supervise any visitors.
- Do not give keys or lock combinations to visitors (or contractors?).
- Require employees to notify management in advance if they wish to gain entry to the computing facility during hours when they are not scheduled to be working.

IT audit trails

To detect computer intrusions, managers can make sure that computer systems maintain an audit trail of access to system resources. Then they can regularly analyse transaction histories, looking for variances from the norm. In addition to checking users' authorisations, managers can pay attention to unusual times, frequency, and length of access.

Paper Information Security

Depending on the threat level, the following methods can be considered:

- Lock file cabinets and trash bins.
- Institute a clean desk policy.
- Mark sensitive documents as "confidential."
- Provide employee training and reminders about document security practices.

Section 5 Security Checklist

The checklist below can be adapted to the needs of an individual company based on the outcomes the risk assessment.

Question		YES/NO	Recommendations
Management Issues			
1	Is there someone appointed with overall responsible for security?		
2	Has a clear company security policy been developed and promulgated?		
3	Have we established partnerships with local, state, and federal security, police and public safety agencies, and surrounding communities?		
	Do we need or have access to specialist security support?		
4	Do we have a system for reporting security incidents?		
5	Is security a feature of employee and contractor employment and training?		
6	Do we have a system for investigating suspicious incidents and security breaches?		
7	Do we periodically reassess the site's security situation (threats, vulnerabilities, risks, and countermeasures)?		
8	Are we aware of all relevant security legislation? Do we comply?		
Risk Assessment			
1	Do we have a system to identify, eliminate or reduce physical security risks?		
2	Have we identified all key facility assets?		
3	Have we performed a threats, vulnerability and consequence assessment?		
4	Have we performed a security assessment/gap analysis?		
Site Security			
1	Have we implemented appropriate access control measures, such as signs, secure doors and windows, locks, card-based access control systems, parcel inspection, and control of gates and docks?		

Question		YES/NO	Recommendations
2	Do we have appropriate perimeter protection, using, for example, fences, bollards, trenches, turnstiles, and security lighting?		
3	Do we need security officers, on patrol or at fixed locations? If so, do they have written instructions to direct their activity?		
4	Have we appropriately protected crucial communications equipment and utilities?		
Emergency Plans			
1	Do we have plans to manage any foreseeable physical security emergency?		
2	Have we developed procedures for emergency response and crisis management?		
Supply Chain Security			
1	Have we verified our customers are legitimate and their use for our product(s) is legitimate?		
2	Do we know the carriers?		
3	Do we have a system to check that only scheduled deliveries are accepted?		
4	Are vehicle access points controlled to prevent 'tailgating'?		
5	Supplier - Do we supply any chemicals that may be diverted for criminal or terrorist activities or are listed in the UN Model Regulations 'High Consequence' list?		
6	Supplier – do we have procedures to prevent the possible misuse of any such chemicals?		
7	Transport operator - Do we have a security plan or procedures in place to address possible threats to our business?		
IT and Information Security			
1	Do we have a system to protect operational information that could be of use to our adversaries?		
2	Are we using appropriate hardware, software, and procedural techniques for protecting our computers and networks?		
3	Do we periodically analyse computer transaction histories to look for irregularities that might indicate security breaches?		
4	Do we follow appropriate procedures for protecting sensitive (paper) documents?		

Section 6 Sources of Information

- **PACIA's Website**
  http://www.pacia.org.au
  Information can be found here on regulatory bodies, regulatory schemes, conventions and treaties, chemical security, diversion to illicit drugs and security sensitive ammonium nitrate (SSAN).

- **Australian Government's National Security Website:**
  www.nationalsecurity.gov.au

- **Attorney Generals Department:**
  http://www.australia.gov.au/chemicalsecurity
  http://www.chemicalsecurity.gov.au/

- **ASIO Business Liaison Unit (BLU)**
  http://www.blu.asio.gov.au/

- **Australia's National Authority for the Chemical Weapons Convention**
  http://www.dfat.gov.au/cwco/

- **Critical Infrastructure Protection**
  http://www.ag.gov.au/www/agd/agd.nsf/page/Nationalsecurity_CriticalInfrastructureProtection

- **The Trusted Information Sharing Network for Critical Infrastructure Protection**
  http://www.tisn.gov.au/

- **State and Territory Counter Terrorism Websites**
  - New South Wales
  - Victoria
  - Queensland

Appendix A

Chemical Security Management Framework

The Report on the Control of Chemicals of Security Concern was developed as part of a national review of the regulation, reporting and security surrounding the storage, sale and handling of hazardous materials.

In October 2008, The Council of Australian Governments (COAG) endorsed this report and agreed to the establishment of a Chemical Security Management Framework that will guide the national approach for managing chemicals of security concern.

The framework comprises:

- Coordination and consultation arrangements between and within governments and industry
- A process for ongoing assessment and management of security risks associated with the use of chemicals for terrorist purposes and;
- The development of capability building measures for community, industry and governments.

The Attorney Generals Department established a Chemical Security Branch in 2008 to coordinate the national implementation of the framework, to undertake risk assessments for the chemicals of security concern and to support the building of capability in government, industry and community.

Chemicals Assessed as of immediate potential security concern

Only chemicals known to be of credible interest to terrorists were considered under the COAG process, which was agreed to in October 2008. Of the 40,000 chemicals in use in Australia, 96 were identified as being of immediate potential security concern.

The Attorney Generals Departments has developed a security risk assessment methodology for the identified chemicals of security concern. This methodology is in line with Australia and New Zealand Standard 4360:2004 and AS/NZS HB 167:2006.

Further information on the activities of the Attorney Generals Department and more generally on chemical security can be obtained at http://www.chemicalsecurity.gov.au/

Chemicals assessed as of immediate potential security concern

A	CAS #	E	CAS #	O	CAS #
Aldicarb	116-06-3	Endosulfan	115-29-7	Omethoate	1113-02-6
Ammonia (anhydrous)	7664-41-7	Ethion	563-12-2	Osmium tetroxide	7446-13-1
Ammonium nitrate*	6484-52-2	Ethyl mercury chloride	107-27-7	Oxamyl	23135-22-0
Ammonium perchlorate	7790-98-9	Ethyldiethanolamine	139-87-7		
Arsenic pentoxide	1303-28-2			P	
Arsenic trioxide	1327-53-3	F		Paraquat	2074-50-2
Arsine	7784-42-1	Fenamiphos	22224-92-6	Parathion methyl	63653-66-7
Azinphos methyl	86-50-0	Fluorine gas	7782-41-4	Perchloric acid	7601-90-3
		Fluoroacetic acid	144-49-0	Phorate	298-02-2
B		Fluoroethyl alcohol	000371-62-0	Phosgene	75-44-5
Bendiocarb	22781-23-3	Fluoroethyl fluoroacetate	459-99-4	Phosphide Al	8005-48-9
Beryllium sulphate	13510-49-1			Phosphide Mg	12057-74-8
Bromine	7726-95-6	H		Phosphide Zn	12037-79-5
		Hydrochloric acid	7647-01-0	Phosphine	7803-51-2
C		Hydrogen chloride	7647-01-0	Phosphorus	7723-14-0
Cadusafos	95465-99-9	Hydrogen cyanide	74-90-8	Phosphorus oxychloride	39380-77-3
Carbofuran	1563-66-2	Hydrogen peroxide	8007-30-5	Phosphorus pentachloride	10026-13-8
Carbon disulphide	75-15-0	Hydrogen sulfide	7783-06-4	Phosphorus trichloride	37231-52-0
Carbon monoxide	630-08-0			Potassium chlorate	7790-93-4
Chloropicrin	76-06-2	M		Potassium nitrate	96193-83-8
Chlorfenvinphos	470-90-6	Mercuric chloride	7487-94-7	Potassium perchlorate	7778-74-7
Chlorine gas	7782-50-5	Mercuric nitrate	8046-70-6	Propoxur	114-26-1
Cyanide calcium	592-01-8	Mercuric oxide	8028-34-0		
Cyanide mercury	592-04-1	Mercurous nitrate	7782-86-7	S	
Cyanide potassium	151-50-8	Methamidophos	115182-35-9	Sodium azide	26628-22-8
Cyanide sodium	143-33-9	Methidathion	950-37-8	Sodium chlorate	7775-09-9
Cyanide zinc	557-21-1	Methiocarb	716-16-5	Sodium fluoroacetate	62-74-8
Cyanogen bromide	506-68-3	Methomyl	16752-77-5	Sodium perchlorate	7601-89-0
Cyanogen chloride	506-77-4	Methyl fluoroacetate	453-18-9	Sodium nitrate	7631-99-4
		Methyldiethanolamine	105-59-9	Strychnine	6899-11-2

		Mevinphos	7786-34-7	Sulfur dichloride	39461-36-4
				Sulfur monochloride	12771-08-3
	333-41-5			Sulphuric acid	7664-93-9
D	62-73-7	N	78989-43-2		
Diazinon	762-04-9	Nitric acid	90880-94-7	T	
Dichlorvos	868-85-9	Nitric oxide	75-52-5	Terbufos	13071-79-9
Diethyl phosphite	593-74-8	Nitromethane		Thallium sulfate	87993-82-6
Dimethyl phosphite	77-78-1			Thionyl chloride	7719-09-7
Dimethyl mercury	298-04-4			Thiophosphoryl chloride	3982-91-0
Dimethyl sulphate				Triethanolamine	7376-31-0
Disulfoton				Triethyl phosphite	122-52-1
				Trimethyl phosphite	121-45-9

* security-sensitive ammonium nitrate (SSAN) [ammonium nitrate, ammonium nitrate emulsions and ammonium nitrate mixtures containing greater than 45 per cent ammonium nitrate, excluding solutions]

Note: CAS means the Chemical Abstracts Service, a division of the American Chemical Society

APPENDIX B

RISK MANAGEMENT MODEL – D^3R^2

The amount of security you need will be determined by determining what your threat is, the vulnerabilities that exist in your facilities, the likelihood of an attack, and the consequences should an attack occur at your facility.

A simple framework for the treatment of security risks is outlined below. It is designed to allow companies to develop layers of protection in their security plans. The phases of this framework are:

- **Deterrence:** is the prevention of action through a fear of unacceptable consequences. Examples are lighting, design, environmental design of facilities, labelling of equipment,

- **Detection:** is the determination and transmission that an event has occurred. The use of technology increases the capability to detect. Examples are access control systems, CCTV (with recover), movement detection.

- **Delay:** is the ability of physical or psychological barriers to restrict movement. The purpose of delay is to allow time for an appropriate response and to make it undesirable for the perpetrator to continue. Examples are fences, locked gates barriers, security of intellectual property.

- **Response:** is the level of reaction required to counter an intrusion. Response forces range from unarmed security guards or staff to local police. Examples are guards, police support, and communications.

- **Recover:** is the ability to ensure that operations can continue. Examples include contingency planning to oppose or negate the effects of an overt or covert action.

Appendix C

Supply Chain Customers

The Council of Australian Governments (COAG) has identified chemicals that have the potential to be illegally diverted for terrorist use. (**My Company**) is supplying (**Chemical X)** a product that meets these criteria.

The information outlined below may be helpful in controlling this risk.

PACIA and its members recognise the importance of ensuring the safety and security of our products through the supply chain.

To be successful in preventing terrorist attacks, we need:

- ***Education and awareness*** of the potential for some specific chemicals to be illegally used (in particular those priority chemicals listed above as well as the full list of 96 identified by COAG, those covered by the Chemical Weapons Convention, and explosives),
- ***Reporting*** of any suspicious behaviours and unaccounted losses, and
- ***Physical security*** to control access.

Know your customer

It is important to know your customer. The following indicators of suspicious behaviour may be useful:

- *A new customer*
- *A 'walk-in' customer (personal appearance)*
- *An offer to pay an excessive price for certain chemicals or apparatus for rapid delivery*
- *Cash payments, even for large purchases*
- *Requests to have the merchandise delivered in non-commercial or unmarked packaging*
- *Purchases in small containers even when industrial use is claimed*
- *Irregular ordering patterns and unusual quantities ordered*
- *Orders or purchases by persons or companies with no obvious need for these chemicals*
- *Indications of intended use that is inconsistent with the chemical ordered*
- *Merchandise that is collected with the purchaser's own vehicle*
- *Request for delivery by air freight*
- *Delivery to a post office box or other incomplete address*
- *Failure or unwillingness to supply a telephone number or an address*
- *Lack of business acumen and absence of standard business stationery*
- *Reluctance to supply a written order*
- *Orders for more than one precursor chemical*

- *Orders to universities or well-known companies where the normal arrangements for ordering are used but delivery is requested to a specific individual*
- *Orders to companies which are not known and cannot readily be traced in trade directories*
- *Orders for chemicals with delivery instructions where the cost of delivery or routing exceeds the cost of the merchandise.*

It is essential that you are comfortable that the product is being received by a legitimate and responsible user.

Unaccounted Losses

Detection of stock loss will allow organisations to detect theft, removal or unauthorised diversion of chemicals of security concern.

Organisations should investigate any potential losses and if irregularities cannot be accounted for, promptly report to authorities to allow investigations to commence.

It is important that clear systems are in place to ensure any suspicious incidents or behaviours or security breaches are reported immediately to the *National Security Hotline on 1800 123 400* *or to the police in accordance with your local arrangements.*

SAMPLE CHECKLIST FOR CUSTOMERS/SUPPLY CHAIN

Question	YES/NO	Recommendations
Management Issues		
Do you have a system for reporting security incidents?		
Do you have a system for investigating suspicious incidents and security breaches?		
Do you periodically reassess the site's security situation (threats, vulnerabilities, risks, and countermeasures)?		
Site Security		
Have you implemented appropriate access control measures, such as signs, secure doors and windows, locks, card-based access control systems, parcel inspection, and control of gates and docks?		
Do you have appropriate perimeter protection, using, for example, fences, bollards, trenches, turnstiles, and security lighting?		
Supply Chain Security		
Have you verified our customers are legitimate and their use for our product(s) is legitimate?		
Do you know the carriers?		
Do you have a system to check that only scheduled deliveries are accepted?		
Are regular stock checks undertaken to detect theft, removal or unauthorised diversion of chemicals of security concern		
Supplier - Do you supply any chemicals that may be diverted for criminal or terrorist activities?		
Supplier – do you have procedures to prevent the possible misuse of any such chemicals?		
Transport operator - Do you have a security plan or procedures in place to address possible threats to our business?		

Plastics and Chemicals Industries Association

Contact us:

National Office

Level 1,
Unit 7 Skipping Girl Place
651 Victoria Street
Abbotsford
VICTORIA 3067

PO Box 211
Richmond
VICTORIA 3121

Phone: +61 3 9429 0670
Fax: +61 3 9429 0690
Email: info@pacia.org.au
Website: www.pacia.org.au

Canberra Office

Phone: +61 2 6230 6985
Fax: +61 2 6230 6714

New South Wales Office

Phone: +61 2 9438 2273

For further details of representatives in particular states, please contact the PACIA National Office.