

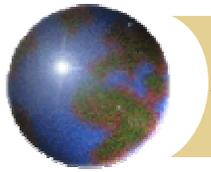
Security and Health Safety

CANADIAN BIOSECURITY SYMPOSIUM 2002

"An Integrated Approach to Security"

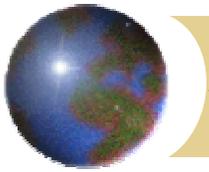
Presented By: Ivan Sicard

Safety, Emergency and Security Management Division, Health Canada



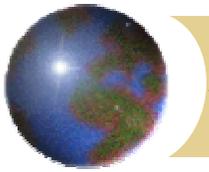
The Challenge

The design and implementation of a laboratory security program based upon the requirement to address unique security threats towards employees, facilities and sensitive information and assets, which in some cases have national interest implications.



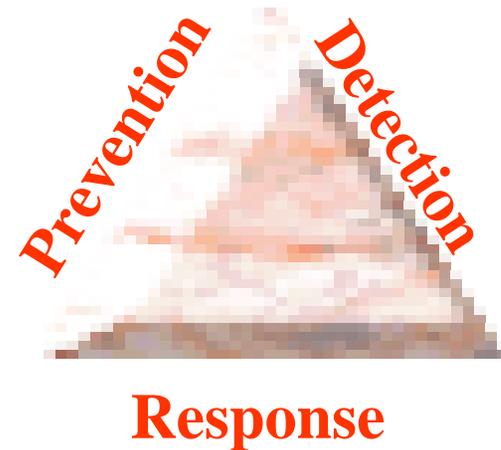
Security Program Mandate

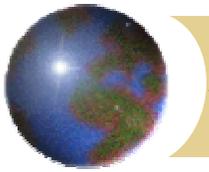
To provide direction, support and assistance to managers and employees in providing a safe and secure work environment in accordance with all applicable Federal, Provincial and other policy and legislative requirements.



Security Program Objectives

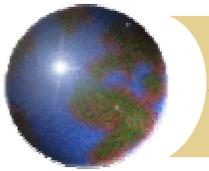
- Establish a level of security sufficient to protect employees, information and assets
 - Safe and secure work environment
 - Effective asset protection
 - Safeguarding of information
 - Prevention and mitigation of losses
 - Maintenance of essential services
 - Critical infrastructure protection
 - Address unique threat requirements (e.g animal research, pathogen transfer)





Today's Security Challenges

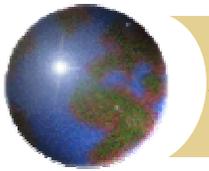
- Maintaining a Safe Workplace
- Criminal Activity
- Espionage
- Compromise of Information
- Protection of Sensitive Assets (e.g pathogens)
- Workplace Violence
- Demonstrations and Occupations
- Disaster Readiness and Building Emergency Response Planning
- Security Awareness and Compliance
- Terrorism



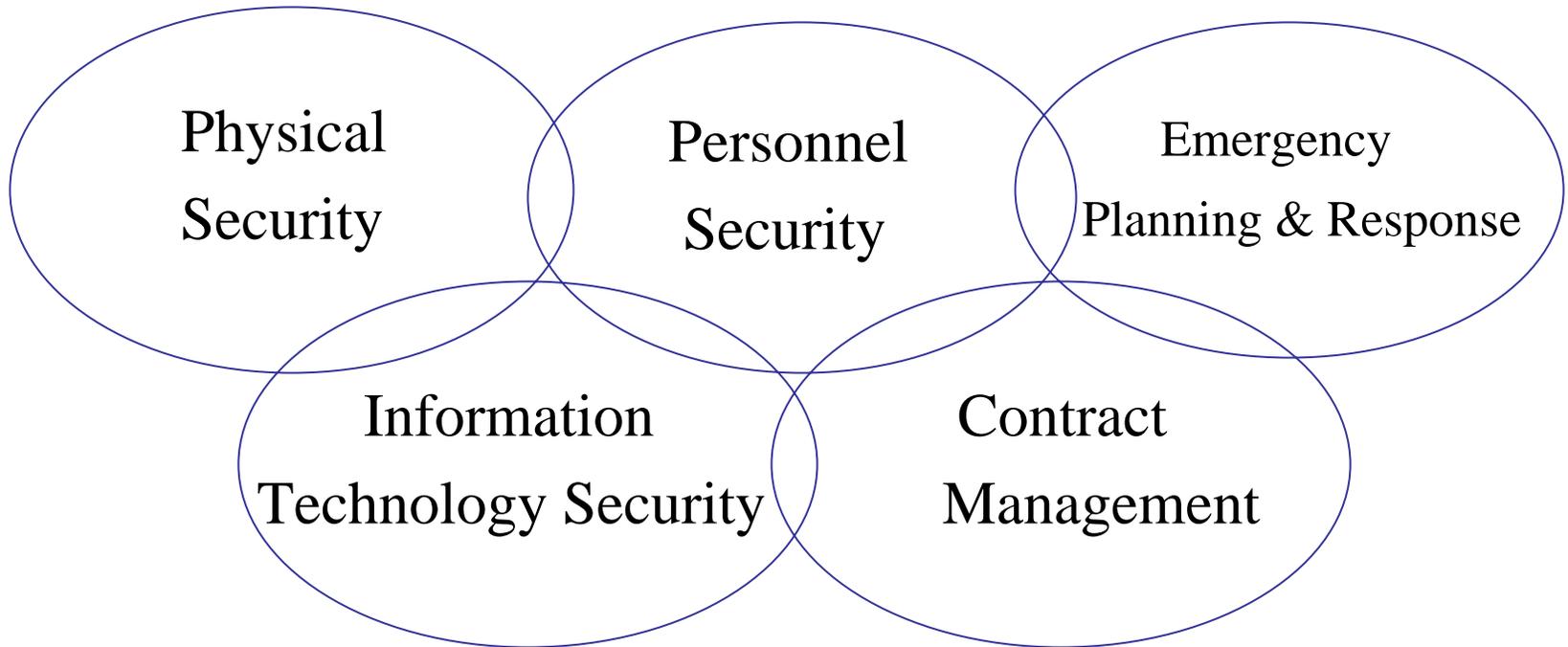
Integrated Systems Approach

(What does it mean ?)

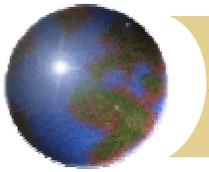
It is the process of achieving effective security management by incorporating several security processes and systems (e.g physical security and employee screening) under an organization and management framework.



Integrated System Approach

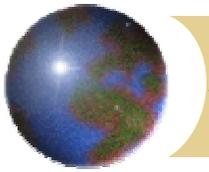


Security Organization and Administration



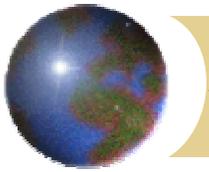
Security Organization & Management

- Security management framework based upon industry best practices
- Senior management commitment
- Security responsibility delegation
- Facility security manager
- Security and guard force personnel
- Management tools, policies and procedures
- Integrated security management framework



Security Organization & Management

- Security Programs based upon Threat & Risk Assessment findings
- State of the art electronic security systems and software
- Security education and awareness program
- Program maintenance and monitoring



Security Design Concepts

Degrees of Protection

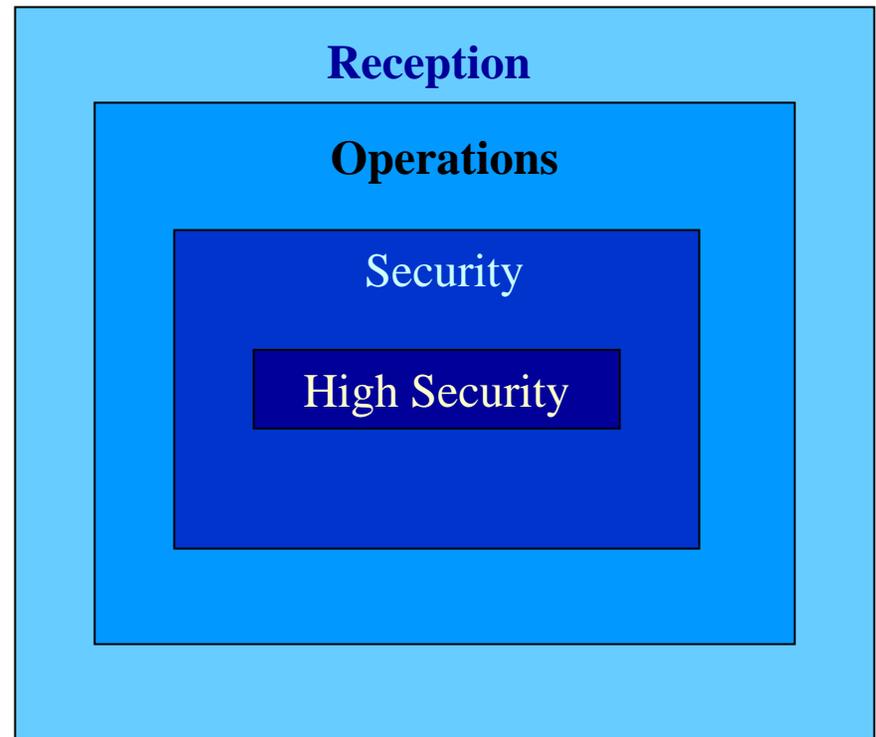
Safeguards

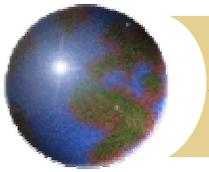
- Electronic security systems
- Access Controls
- Doors, walls & windows
- Locking hardware
- Exterior Fencing
- SOP's
- Security Screening
- Employee Awareness
- Guard Force

Physical Security

Strategies

- Target Hardening
- Protection, Detection & Response





Threat & Risk Assessment

1. Identification of assets → information → material → equipment

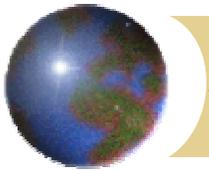
2. Identification of threats → removal, interruption, modification, destruction, disclosure

3. Likelihood of occurrence $\begin{matrix} \overline{H} \\ | \\ M \\ | \\ L \end{matrix}$ = priority for action → in terms of consequences

4. Evaluation of safeguards

5. Recommendations

Breach of security	- legal action
Effect on country	- personal injuries
Effect on institution	- time loss
Effect on activities	- financial impact
Violation of GSP	



Threat & Risk Assessment

Assets

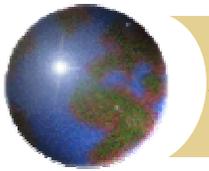
- personnel/occupants
- designated & classified information
- labs, lab equipment, experiments, animals & animal facilities, special pathogens (bacterial viral), building mechanical & information management systems

Location

- dependent on sensitivity: assets will be stored in operations, secure or high security zones and/or containers in a secure or high security zone

Risk Probability

- planned security safeguards will bring risk probability of identified threats being realized to low/medium range



Threat & Risk Assessment

Threat

Vandalism (Outsider)

Vandalism (insider)

Break & Enter

Trespassing (Outsider)

Demonstrations

Theft (outsider/insider)

Assault (inside/outside building)

Sabotage (outsider/insider)

Unauthorized access or
disclosure of information

Probability

med

low

low/med

med

med

low/med

low/med

low

low

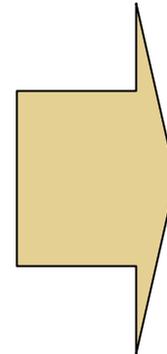
Consequences

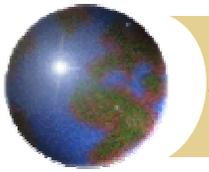
not too

serious to

exceptionally

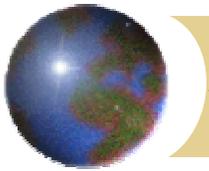
grave





Threat & Risk Assessment

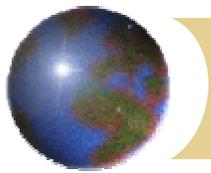
- Primary threat perpetrators
 - Persons/groups intent on committing criminal activity towards facility, assets or occupants



Personnel Security Screening Program

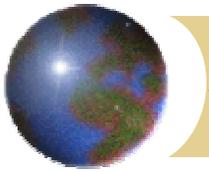
Purpose

- Ensure all persons (employees, contractors, students, agency personnel, visitors, consultants, foreign visiting scientists etc.) with access to sensitive information and assets are security screened/cleared to the appropriate level.



Personnel Screening

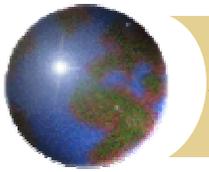
- Ensure security screening/clearances & employee background checks are obtained for all persons under your management
- Address adverse information, conduct subject interviews where required
- Issue ID cards to authorized employees, contractors, visitors, limit access to space, information and assets on need to know need to access basis only
- Complete Arrival/Departure Form for new and departing employees
- Immediately report missing ID cards



Physical Security Program

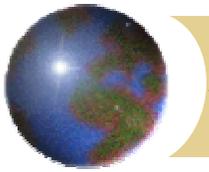
Purpose

- To provide advice, consultation and security services for the protection of personnel, information and assets.



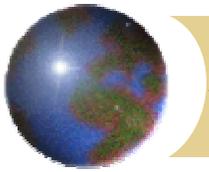
Physical Security Program

- Security Threat and Risk Assessment Process
- Physical Security Consultation & Security Operations Services
 - ◆ Design Briefs, Relocations, Security Zones, Secure Rooms
 - ◆ Security Equipment and Systems (alarms, access controls, locks, doors, windows, etc.)
 - ◆ Document and Asset Safeguarding
 - ◆ Incidents and Investigations
 - ◆ Building Access Control
 - ◆ Guard Force Operations, Alarm Monitoring & Response
 - ◆ Door/lock Combination Registration & Changes
 - ◆ 24/7 Security Emergency Operations Centre



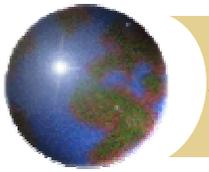
Physical Security Program (Cont'd)

- Ensure employees comply with the physical security requirements for control and accountability of assets within your respective areas
- Ensure employees comply with all requirements of building access control policies and procedures
- Ensure all security incidents are reported to Facility Security Manager



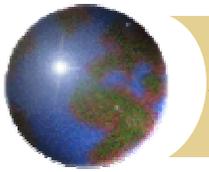
Physical Security Program (Cont'd)

- Invite key facility managers and security personnel to be part of the project team to address the security requirements for special events, relocations, retrofits, enhancements and for building of new facilities
- Identify and implement appropriate security measures to protect unique or valuable assets

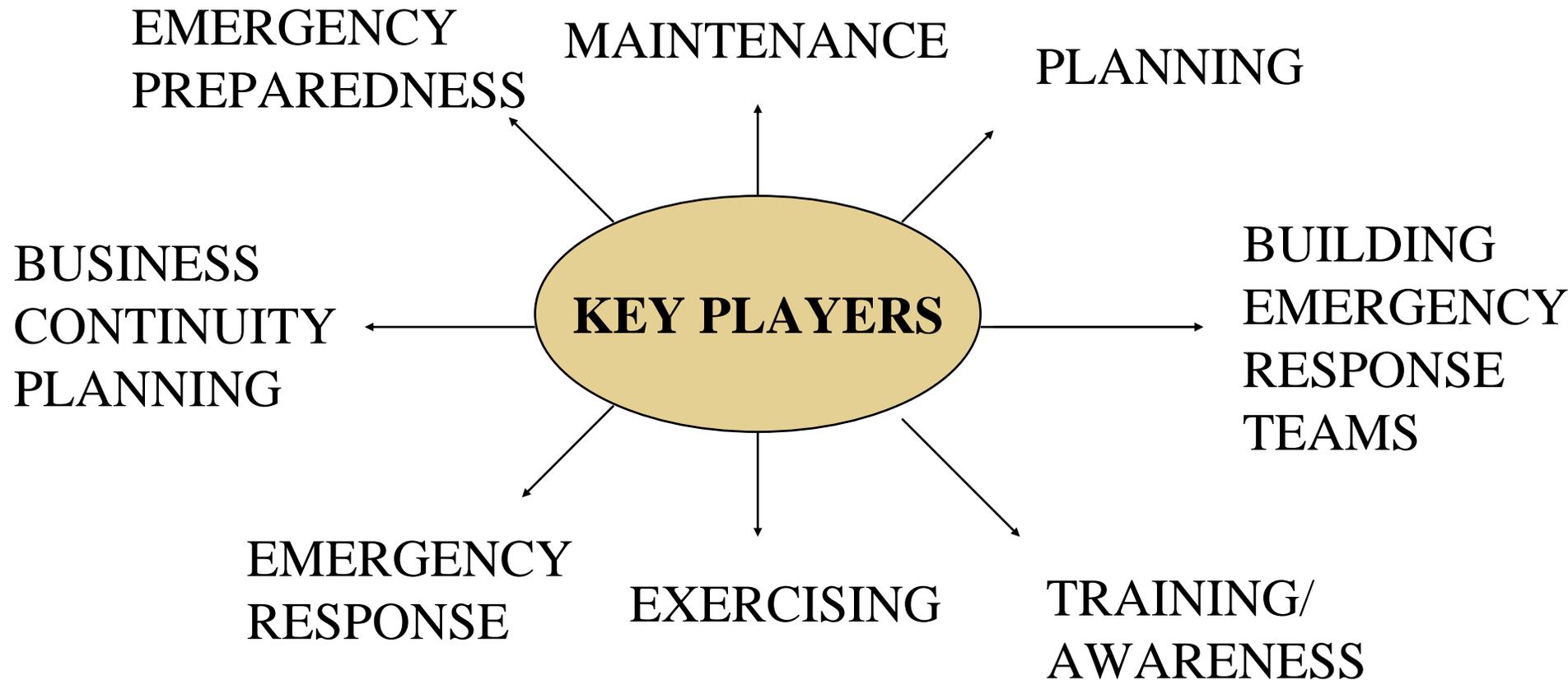


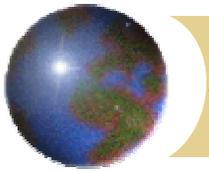
Building Emergency Response Planning Purpose

- To assist the employer in meeting their legislated obligations to develop workplace specific emergency response plans. These plans ensure the safety of employees and visitors and provide for the protection of assets in the event of a threatening or emergency situation.



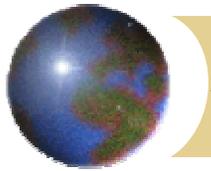
Emergency Response Planning





Building Emergency Response Planning

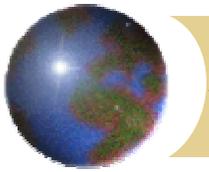
- The employer is responsible for the development of building specific emergency response plans
- This not only ensures the safety of employees and visitors but also provides for the protection of assets and critical infrastructures in the event of a threatening or emergency situation.



Considerations

The lack of emergency preparedness and business continuity planning could result in:

- Mass confusion during emergencies, needless injury, loss of life, damage to property and disruption to business operations
- Lack of Due Diligence can result in serious liability claims towards an organization and its senior employees
- Inability to deliver essential services



Building Emergencies to Plan For

Fire Emergency and Building Evacuations

Suspicious Packages / Bomb Threats

Hazardous Material Incidents

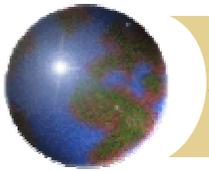
Utility Incidents

Demonstrations and Occupations

Occupational Illness and Injury

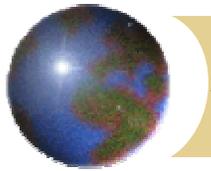
Workplace Violence

Natural Disasters



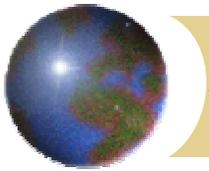
Fire Emergency Organization

- The Fire Emergency organization is the foundation of the emergency response program
- Provides coordinated and efficient means to manage building evacuations during the course of normal working hours
- Conducts fire drills in accordance with applicable legislation
- Report unsafe fire conditions for corrective action



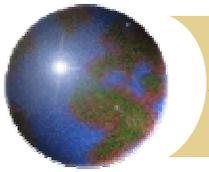
Special Events

- Safety and security advice should be given to organizing committees who require assistance safeguarding personnel, assets, systems or buildings during special events.
- Prepare a security plan
- Liaise with police and intelligence agencies for threat assessment advice



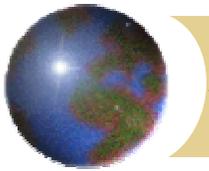
Business Continuity Planning Purpose

- To provide for the continued availability of critical services and assets within the Department



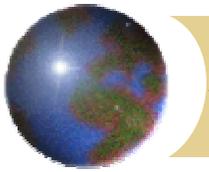
Business Continuity Planning Managers Responsibilities

- Develop a business continuity plan for your area which includes the following:
 - Governance Structure (organization commitment of team)
 - Business Impact Analysis (identify essential services & systems)
 - Plans arrangements (Recovery strategies, manual work-arounds)
 - Readiness (testing & maintenance)



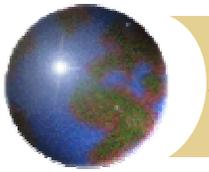
Occupational Health and Safety Program

- Promote a safe and healthy workplace for all employees
- Prevent and reduce accidents, illness and injuries



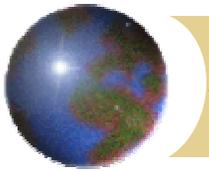
Occupational Health and Safety

- Policy and Guidelines
- OSH Committees
- Responsible Building Authority (RBA) Program
- Awareness, education and training
- First Aid/CPR
- Workers' Compensation Program
- Hazardous Occurrence, Investigation and Reporting



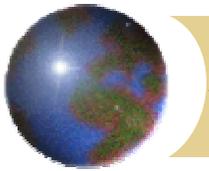
Occupational Health and Safety Managers Responsibilities

- **Regulated to provide a healthy and safe workplace for employees and all others by:**
 - ◆ Familiarizing themselves with their specific duties and responsibilities under the CLC/Provincial Labour Codes
 - ◆ Investigating and reporting all hazardous occurrences and accidents
 - ◆ Complying with standards relating to fire safety and emergency procedures
 - ◆ Providing task specific training to employees (e.g. lab safety requirements)



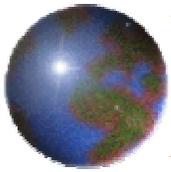
Occupational Health and Safety Managers Responsibilities (Cont'd)

- Communicating to employees every known or foreseeable safety or health hazard
- Ensuring that hazardous substances are identified, stored and handled safely – Workplace Hazardous Materials Information System (WHMIS)
- Providing safety material, equipment and clothing to each person granted access to the workplace
- Providing first aid facilities and health services
- Exercising Due Diligence



Security and Safety Relationship

SECURITY	SAFETY
<p>TBS – GSP</p> <p>Provincial Security Policy</p> <p>RCMP, CSIS, CSE & OCIEP</p> <p>Protection of Occupants and Assets</p> <p>Due Diligence</p>	<p>HRDC, Labour Program</p> <p>Provincial Labour Codes</p> <p>Canada Labour Code</p> <p>Canadian Centre for Occupational Health & Safety</p> <p>Protection of Employees</p> <p>Due Diligence</p>



Other Security Issues for Consideration

- Security Incident Reporting System
- Points of Contact (Police, Fire, EMS, Lead Agencies for Security)
- Investigations
- Security in Contracting
- Special Documents (i.e. Cabinet Docs)
- Asset Control (inventory asset removal form)
- Workplace Violence
- Crime Prevention Through Environmental Design (CPTED)
- Foreign Travel
- Recruiting Good Security People