



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC1005A Apply critical infrastructure protection procedures

Release: 1

CPPSEC1005A Apply critical infrastructure protection procedures

Modification History

Not Applicable

Unit Descriptor

Unit descriptor This unit of competency specifies the outcomes required to understand the potential risk and associated risk events relevant to the security of national critical infrastructure and procedures. It requires a knowledge and understanding of reporting procedures and the specific personnel who have responsibility for responding to security threats and emergencies.

This unit may form part of the licensing requirements for persons engaged in security operations in those states and territories where these are regulated activities.

Application of the Unit

Application of the unit This unit of competency has wide application in security work roles across a wide range of industry sectors which cover essential services such as power, water, health services, communications systems and banking.

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Not Applicable

Employability Skills Information

Employability skills This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency. Performance criteria describe the required performance needed to demonstrate achievement of the element. Where ***bold italicised*** text is used, further information is detailed in the required skills and knowledge section and/or the range statement. Assessment of performance is to be consistent with the evidence guide.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1 Identify legislative and organisational requirements.	1.1 Basic <i>legislative</i> and <i>organisational requirements</i> relevant to the security of <i>critical infrastructure</i> are identified and explained. 1.2 <i>Duty of care requirements</i> are identified and explained. 1.3 Own level of authority, role and responsibilities are identified and explained. 1.4 Role and responsibilities of <i>designated personnel</i> responsible for responding to security threats and emergencies are identified and explained. 1.5 <i>Occupational Health and Safety (OHS) requirements</i> are identified and explained.
2 Identify potential threats.	2.1 Range of <i>critical infrastructure sectors</i>, facilities and services are identified and explained. 2.2 Types of <i>risk and associated risk events</i> are identified and explained. 2.3 <i>General procedures for monitoring security</i> of the work environment are identified and explained. 2.4 <i>Indicators of terrorist activity</i> are identified and explained. 2.5 Emergency and evacuation procedures are identified and explained. 2.6 <i>Appropriate actions for maintaining security and safety</i> of self, others, property and premises are identified and explained. 2.7 <i>Methods for gathering intelligence</i> related to suspected threats or terrorist activity are identified and explained. 2.8 Methods for determining the source of potential threat and the target are identified and explained.
3 Identify threat reporting processes.	3.1 Organisational <i>procedures for reporting</i> suspected threats to critical infrastructure are identified and explained. 3.2 Chain of command of designated personnel is identified and explained. 3.3 Organisational <i>communication channels and processes</i> are identified and explained. 3.4 Types and purpose of <i>communication equipment</i> are identified and explained.

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge and their level required for this unit.

Required skills

- communication and interpersonal skills to:
 - ask effective questions
 - clarify security procedures
 - give accurate verbal or written descriptions of potential security risks and threats and appropriate reporting procedures
 - interpret selected pictorial, graphical and written signs and instructions
 - relay information to others.
- comprehension skills to:
 - explain the basic legislative and organisational requirements which will be applicable to own work environment and role
 - explain the difference between terrorist activities and other security risks
 - explain the general methods for gathering intelligence related to suspicious behaviour or activity
 - explain the general procedures for maintaining security and safety of self and others in the event of suspected security risk or incident
 - explain the range of critical infrastructure sectors, facilities and services provided
 - explain the range of indicators of potential terrorist activities
 - explain the procedures for reporting identified security risks
 - explain the types of risk and associated risk events relevant to critical infrastructure.

Required knowledge

- applicable commonwealth, state or territory legislation relevant to own work environment and role including use of force guidelines
- applicable OHS requirements
- communication modes and equipment relevant to the workplace
- duty of care requirements
- general methods for observing incidents and monitoring risks within the work environment
- general procedures for emergency, evacuation and first aid response
- general procedures for reporting identified suspicious behaviour and activity
- organisational requirements relevant to own work role and responsibilities
- reporting chain of command
- role of designated personnel responsible for responding to security threats and emergencies
- types of national critical infrastructure and the essential services provided
- types of security risk and associated risk events relevant to national critical

REQUIRED SKILLS AND KNOWLEDGE

infrastructure facilities and services

- unique nature of terrorism as distinct from criminal incidents.

Evidence Guide

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Critical aspects for assessment and evidence required to demonstrate competency in this unit

A person who demonstrates competency in this unit must be able to provide evidence of understanding and knowledge of the following:

- applicable basic legislative, organisational and OHS requirements relevant to security protection including duty of care requirements, and own role and authority
- appropriate actions to maintain security and safety of self, others, property and premises including general procedures for emergency, evacuation and first aid response
- procedures for reporting suspicious behaviour or activity to designated personnel including the use of appropriate communication equipment, channels and processes
- the types of national critical infrastructure and potential security risks to the essential services they provide.

Context of and specific resources for assessment

Context of assessment includes:

- a setting in the workplace or environment that simulates the conditions of performance described in the elements, performance criteria and range statement.

Resource implications for assessment include:

- access to a registered provider of assessment services
- access to a suitable venue and equipment
- access to plain English version of relevant statutes and procedures
- assessment instruments including personal planner and assessment record book
- work schedules, organisational policies and duty statements.

Reasonable adjustments must be made to assessment processes where required for people with disabilities. This could include access to modified equipment and other physical resources, and the

provision of appropriate assessment support.

Method of assessment This unit of competency should be assessed using questioning of underpinning knowledge and skills.

Guidance information for assessment Assessment processes and techniques must be culturally appropriate and suitable to the language, literacy and numeracy capacity of the candidate and the competency being assessed. In all cases where practical assessment is used, it should be combined with targeted questioning to assess the underpinning knowledge.

Oral questioning or written assessment may be used to assess underpinning knowledge. In assessment situations where the candidate is offered a choice between oral questioning and written assessment, questions are to be identical.

Supplementary evidence may be obtained from relevant authenticated correspondence from existing supervisors, team leaders or specialist training staff.

Range Statement

RANGE STATEMENT

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Legislative requirements may relate to:

- anti-terrorism
- applicable Crimes Acts or Codes
- Australian standards, quality assurance and certification requirements
- award and enterprise agreements
- general 'duty of care' responsibilities
- powers and procedures for effecting an arrest
- privacy
- relevant commonwealth, state and territory legislation which affect organisational operation:
 - anti-discrimination and diversity
 - environmental issues
 - equal employment opportunity
 - industrial relations

Organisational requirements may relate to:

- OHS
- relevant industry Codes of Practice
- security licensing or certification
- use of force.
- access and equity policy, principles and practice
- client service standards
- code of conduct
- code of ethics
- communication channels and reporting procedures
- emergency and evacuation procedures
- employer and employee rights and responsibilities
- licensing
- OHS policies, procedures and programs
- organisational goals, objectives, plans, systems and processes
- policies and procedures relating to own role, responsibility and delegation
- reporting systems, procedures and processes.

Critical infrastructure:

- are physical facilities, supply chains, information technologies and communication networks that if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security.
- provides essential services such as power, water, health services, communications systems and banking.
- may relate to own responsibilities to comply with safe working practices including activities which require licences or certificates of competency
- relate to the legal responsibility under "duty of care" to do everything reasonably practicable to protect others from harm.

Duty of care requirements:

Designated personnel may include:

- emergency services
 - ambulance
 - Australian Defence Force personnel
 - fire services
 - rescue
 - police
- first aid officer
- government representatives
- security personnel
- supervisor.

Occupational Health and Safety (OHS) requirements may include:

- controlling and minimising risks
- correct manual handling including shifting, lifting and carrying
- first aid
- identifying and reporting hazards and risks
- knowledge of emergency and evacuation procedures
- transporting and storing dangerous goods
- using and maintaining equipment
- using and maintaining personal protection equipment
- using and storing hazardous materials and substances.

Critical infrastructure sectors include:

- communications
 - electronic mass communications
 - postal services
 - telecommunications (phone, fax, Internet, cable, satellites)
- energy
 - electricity generation and transmission
 - gas
 - petroleum fuels
- essential manufacturing
 - chemicals
 - defence industry
 - heavy industry
- finance
 - banking
 - insurance
 - trading exchanges
- food supply
 - bulk production
 - storage and distribution
- government services
 - defence and intelligence facilities
 - emergency services (police, fire, ambulance etc)
 - foreign missions
 - houses of parliament
 - key government departments
 - key residences
 - nuclear facilities
- health
 - hospitals

- public health
- research and development laboratories
- national icons
 - buildings
 - cultural
 - sport and tourism
- transport
 - air
 - inter-modal (cargo distribution centres)
 - rail
 - road
 - sea
- utilities
 - water
 - waste management
 - waste water.
- chemical, biological and radiological threats to water and food supplies
- criminal activity
 - assault of people
 - break and enter
 - theft of assets
- e-crime
 - computer hackers
 - viruses
- group interference and damage eg violence prone groups, politically motivated or otherwise
 - major interference to services and transport operations
- insider interference by disgruntled employees, contractors etc
 - interference to services
 - theft or sabotage of critical equipment and infrastructure
- natural disasters
- public interference, disturbances and delays by intoxicated persons, persons in custody, mentally or emotionally disturbed person and irate customers
- terrorism
 - bombings
 - kidnappings
 - sabotage

Risk and associated risk events may include:

General procedures for monitoring may include:

- shootings
- vandalism
- damage to transport conveyances and equipment.
- following designated organisational procedures
- maintaining vigilance and awareness of security while at work
- observing crowd and individual behaviour
- observing suspicious activity
- observing vehicle movement
- recording details of observed risk situations.

Terrorist activity may relate to:

- bombs or other explosions
- kidnap and abductions
- spill or release of toxic chemicals or biological substances
- suicide bombing
- suspicious items received by mail
- unattended packages or other items.

Indicators of terrorist activity may include:

- false or multiple identities such as licences and passports
- individuals who:
 - do not fit into the surrounding environment because they are wearing improper attire for the location or season
 - draw pictures, take notes or take photographs in an area not normally of interest to a tourist
 - order food at a restaurant and leave before the food arrives or who order without eating
 - sit in a parked car for an extended period of time
 - stay at bus or train stops for extended periods while buses and trains come and go
- multiple sightings of the same suspicious person, vehicle or activity, separated by time, distance or direction
- show unusual interest in or photograph security cameras or guard locations
- suspicious accommodation needs
- suspicious activity, especially when connected with a high risk or symbolic target
- suspicious vehicles near significant buildings or in busy public places
- unattended bags and packages
- unusual rentals, purchases, deliveries or thefts, particularly of poisonous or flammable chemicals, fertilisers, explosives, weapons or vehicles eg including planes or boats
- unusual requests for information, particularly about

- security or procedures for at-risk buildings or activities
 - unusual videotaping or photography of official buildings or other critical infrastructure.
- Appropriate actions for maintaining security and safety may relate to:***
- evacuation
 - notifying designated personnel
 - request for assistance
 - tactical withdrawal.
- Methods for gathering intelligence may include:***
- observing and recording details of relevant persons
 - approximate age
 - build eg medium, heavy set, thin etc
 - clothing
 - hair eg colour, length, facial hair etc
 - height
 - method of escape eg direction, vehicle etc
 - peculiarities eg scars, tattoos, missing limbs etc
 - race
 - sex
 - weight
 - observing and recording details of vehicles:
 - body type eg two-door, four-door, van, 4 wheel drive etc
 - damage or other feature eg logo
 - licence plate
 - passengers
 - year, make, model and colour
 - observing and recording other suspicious activity.
- Procedures for reporting suspected terrorist activity may include:***
- completing documentation such as logs, journals and activity reports
 - completing police reports
 - completing written and computer reports
 - contacting designated personnel
 - recording observed intelligence
 - requesting assistance.
- Communication channels and processes may relate to:***
- direct line supervision paths
 - established communication protocols
 - formal communication pathways
 - lateral supervision paths
 - organisational communication networks
 - verbal and non-verbal communication procedures
 - call signs

- coded messages
 - hand signals
 - phonetic alphabet
 - pro-words
 - use of abbreviations.
- Communication equipment may include:**
- pager
 - portable and mounted two-way radio
 - public address system
 - telephone
 - telephone and mobile telephone.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Operations