Dams Safety Committee

NEW SOUTH WALES

DSC2H June 2010

DAM SECURITY

Table of Contents

Item **Page**

1. Introduction 2

2. DSC Security Goal and Key Requirements 2

3. Background 3

4. Security Evaluation 4

5. Reporting 7

6. Security Design and Implementation 7

7. Security Operation, Maintenance & Review 8

8. Documentation 10

9. References and Sources 11

1. INTRODUCTION

The *normal requirements* of the Dams Safety Committee (DSC) are set out in its guidance sheets with its principal guidance sheet, *DSC Background, Functions and Operations - DSC1A,* outlining the DSC's general operations and authority.

The DSC continues to give critical consideration to the security, from interference, of prescribed dams in NSW. The purpose of this guidance sheet is to provide the owners of prescribed, or proposed, dams with general advice on good dam's security practice, along with specific advice on their responsibilities and the requirements of the DSC in this area.

The DSC Security Goal and Key Requirements (Section 2) at the start of the sheet are a summary - the whole sheet is to be read for a proper understanding of DSC considerations on security for dams.

2. DSC SECURITY GOAL AND KEY REQUIREMENTS

2.1 DSC Security Goal

The goal of the DSC regarding security of prescribed dams is to ensure that the likelihood of dam failures, or other dam incidents, from security breaches is low enough to result in tolerable risks to community interests. This goal has shaped the DSC's approach to regulation of security measures as set out in Table 1.

Table 1 - DSC Approach to Dam Security Regulation

Regulated by DSC		**Not regulated by DSC**	
Measures to avoid a prompt failure of a dam with significant consequences for community interests.	Measures to avoid unauthorized operation of spillway / control systems that would have significant consequences for community interests.	Measures to protect against security breaches that do not involve prompt dam failure or unauthorized operation of spillway / control systems without significant flooding.	Measures to protect against vandalism, damage or interference to dam facilities where there is no significant risk to community interests.
Examples: 1. measures to prevent unauthorized truck or heavy equipment access to a dam 2. measures to prevent unauthorized persons obtaining *as built* drawings of a dam.	Examples: 1. measures to prevent access to on-site gate operating systems 2. measures to prevent unlawful access to remote computers controlling spillway gates.	Examples: 1. measures to protect against poisoning of water supplies 2. measures to protect against opening of storage release valves.	Examples: 1. measures to prevent damage to monitoring equipment that can be easily and rapidly repaired 2. measures to protect against damage to a dam that cannot release stored waters.

It is for the dam owner to determine how the goal will be achieved and to demonstrate to the DSC that the goal is achieved or will be achieved following appropriate action(s). The following sections of this sheet aim to provide guidance to assist the owner in the achievement of the DSC's goal.

2.2 DSC Key Requirements

This section summarises the DSC requirements outlined in this sheet.

5. REPORTING

The DSC requires dam owners to give an updated qualitative opinion of the security risk status of their dams (including reviews) in each Surveillance Report prepared for their dams (see DSC2C).

8. DOCUMENTATION

The DSC requires dam owners of Significant or higher Consequence Category dams to maintain the following security documentation:

- A risk-based security plan that addresses security arrangements for each dam (for larger organisations this may include both a strategic framework and a site specific plan);
- Current security threat, vulnerability and risk assessments for each dam (some of which may be supplied from external agencies);
- Procedures for reporting security information and responding to security incidents;
- Record of the outcomes of security surveys and reviews on each dam; and
- An O&M Manual for each dam which has a separate section referring to security responsibilities and identifying the location of the above documentation.

The DSC considers that all information detailing security threats, risks, plans and measures should be categorised as STAFF or SECURITY-IN-CONFIDENCE at a minimum. Each dam organisation must define in their information security strategy how they protect this information and who can have access.

3. BACKGROUND

The DSC has statutory functions to ensure that all prescribed dams do not impose an intolerable level of danger to the community's interests. Traditionally, this has involved setting appropriate safety levels for resisting natural events (e.g. floods) as well as ensuring appropriate management practices are instituted to minimise risks during a dam's life. However, in recent years there has been a drive world-wide for increased security, particularly for critical infrastructure, reinforced by Government requirements in this area and the increasing legal emphasis on the law of negligence requiring a high duty of care for dam owners.

Responding to community and government concerns on security, highlighted by the incidents of 11 September 2001, the DSC requested NSW prescribed dam owners in 2002 to review their security arrangements, update their Dam Safety Emergency Plans in this area, and report generally on their dam's security

adequacy in their Surveillance Reports to the DSC. To assist in this regard the DSC listed various references for dam owners' consideration. In addition, federal and state Governments in Australia have subsequently required owners of critical infrastructure, including dams, to implement appropriate security arrangements relative to its vulnerability and criticality.

After consideration of current security appraisal methods and strategies world-wide the DSC has prepared this sheet setting out its normal requirements for, and guidance to, dam owners on dam security matters. In this regard the DSC has adopted, as its basic requirements, the guiding principles set out in the ANCOLD *Guidelines on Dam Safety Management - August 2003* and ANCOLD *Guidelines on Risk Assessment - October 2003*.

4. SECURITY EVALUATION

4.1 General

The DSC stresses that it is important to recognise that dam security should not be treated in isolation, but as part of the holistic security for the entire site covering the storage, catchment area and associated water transfer infrastructure. This is a key principle, despite the DSC regulating only some aspects related to the safety of the dam (Table 1). Some of a dam's best protection may be provided by security-in-depth created through the surrounding land / infrastructure and the security measures employed on them. However, it is acknowledged that this may need to be balanced with community expectations of access in many cases.

Dam owners should cover the following areas in their dam security evaluations:

- **Security Threat Assessment**

This should be all-source (i.e. compiled from all information sources where practical, noting that some classified information may not be available) and it should be all-threat (i.e. it should assess all threat sources, not just terrorism). The assessment of security threat should be undertaken in consultation with the NSW Police. Written assessments may be developed internally or sourced externally through the NSW Police and other agencies as appropriate (e.g. NSW Premiers Department and Commonwealth security agencies). Examples of main generic threat types include physical acts (by terrorists, issue motivated groups or criminals), internal threats and information security threats, including cyber threats to dam operating systems.

- **Vulnerability Assessment**

Security vulnerabilities are weaknesses in the dam, its surrounding environment, or processes related to the dam, or its security, that could be exploited by a threat element. It is important to understand the vulnerabilities that exist as, when they are considered in the context of current security threats, they inform the identification of risk and the assessment of likelihood as part of the security risk assessment process. The assessment should identify the basic requirements or standards relating to the dam's vulnerability to security-related attacks and should relate to

likely areas of dams that may be vulnerable to certain types of attack. Examples of possible vulnerabilities at a dam site include insecure operating systems, physical dam deficiencies and isolation / communication vulnerabilities.

- **Criticality Assessment**

This should assess the criticality of a dam and its ancillary components (e.g. spillway controls) that are important to its function or safety. Criticality is rated qualitatively using criteria that typically includes:

- Potential impacts of any threat against the dam should the threat be successful;
- Organisational and social value of the dam;
- Degree of redundancy that exists in the system;
- Capability and time taken to resume normal operations if the dam is damaged or fails.

Assessed criticality will assist in analysing consequences of risks and may assist in prioritising risk treatment for aspects of the dam and its security. The assessment may occur as part of critical infrastructure protection activities with the NSW Police and other agencies or, for dams not identified as critical under the NSW framework, they may need to be carried out by the owner alone.

- **Security Risk Assessment**

This should follow the principles outlined in the Australian/New Zealand Standard-AS/NZS 4360:2004 *Risk Management* and the Security Risk Management Handbook - AS/NZ HB167:2006. International standard *AS/NZS ISO/IEC 27001:2006 Information Technology – Security Techniques – Information Security Management Systems – Requirements* and the Australian *Information Security Risk Management Guidelines Handbook - AS/NZS HB 231:2004* should also be considered in relation to the protection of information relating to dams. The assessment should analyse the likelihood and consequence of all identified security risks, in the context of existing security controls for the dam.

4.2 Risk Assessment / Index Schemes / Checklists

The risk assessment process for dams is generally embodied in the following risk equation:

(Likelihood of Attack=Threat x Vulnerability) x (Consequence) = Risk

However, there are a variety of variations that produce acceptable risk assessment outcomes. See HB 167:2004 (Reference 15) for examples of commonly used formulae and the benefits the different approaches offer. To assist dam owners to solve the risk equation, various proprietary risk assessment process packages have been, or are being, developed to analyse or benchmark current security risks at dams and to provide information to support effective risk reduction decisions by dam management teams. Useful references for dam owners in this regard are given in the reference section of this Guidance Sheet but overall the process

should comply with the requirements and guidance of AS/NZS 4360:2004 and AS/NZ HB 167:2006.

However all risk assessment processes require consideration of:

(a) Risk Context (i.e. Degree of Security and Controls Required)

Here dam owners need to determine:

- The context in which the risk process is to be carried out (strategic, organisational, environmental, social, etc);
- The risk criteria and process to be followed for the assessment;
- Stakeholders in the assessment process; and
- Current status of security at dam sites, which may include:
    - Public access arrangements for the dam (e.g. from open to restricted to closed access);
    - The degree of infrastructure security at the dam (e.g. from open access to single defence locks to defence-in-depth such as locks, buildings, fences and barriers);
    - Alarm capability at the dam (e.g. from no alarms to access alarms to monitored video surveillance); and
    - Security presence and response at the dam (e.g. from occasional inspections to daily inspections to 24 hour operator on site to 24 hour guards on site).

(b) Risk Identification (i.e. Threat, Vulnerability and Criticality)

Here dam owners need to identify all of the possible security risks to the dam. This is done by considering the threat sources and how they interact with the identified vulnerabilities, in the context of the dams criticality (in terms of both its purpose and public safety).

(c) Risk Analysis

Here dam owners need to estimate the likelihood of the identified risk events to their dams, the consequences of the events and therefore the security risk levels that apply to the dam for each identified risk.

(d) Risk Evaluation

In this phase the owner needs to compare the risks with tolerability criteria. With regard to risks to the welfare or interests of the community, the criteria need to be based on the DSC guidelines on tolerability of risk or otherwise agreed with the DSC. For risk to the owner's business interests, the owner needs to decide on the criteria. The outcome of this phase is a rating of the risks and assignment to broad classes, such as:

- intolerable (risk reduction is required as soon as reasonably practicable);
- not intolerable but risk reduction will be required to achieve risks as low as reasonably practicable (ALARP);
- tolerable (the owner can live with the risks for the time being but needs to keep them under review and further reduce them as opportunity permits);
- negligible (risks so low that effort to seek further risk reduction is not worthwhile though any obvious low cost improvements ought to be made, with allowance for periodic review to ensure circumstances have not increased the risk).

5. REPORTING

The DSC requires dam owners to give an updated qualitative opinion of the security risk status of their dams (including reviews) in each Surveillance Report prepared for their dams (see DSC2C).

6. SECURITY DESIGN AND IMPLEMENTATION

6.1 General

Security at a dam should be viewed holistically and include the three main areas of security being:

- Physical security of the dam and ancillary structures;
- Security of dam owner personnel and the public; and
- Information security.

The DSC considers it important that dam owners recognise some of the basic principles of security when designing and implementing a security system / process for their dam. These include:

- Security-in-Depth which is the foundation of all good security planning and focuses on an integrated multi-barrier approach for security systems;
- Crime Prevention through Environmental Design including consideration of natural surveillance (e.g. no blind areas), natural access controls (e.g. bunding) natural territorial reinforcement (e.g. providing clear boundaries) and maintenance/management activity (e.g. relates to site image); and
- Protective Security Principles of deterrence, detection, assessment, delay and response. All security measures should be evaluated against these functions as, the more they achieve the more valuable the measure is to security.

6.2 Design and Implementation Considerations

Design and implementation of a security management plan or system should be:

- Intelligence driven in that it is relevant to the threat and can be scaled to meet changes in the threat; and

- Risk driven in that it needs to be prioritised to treat the highest risk areas and that it can also balance the security risks against risk associated with effective operation and public confidence / reputation.

Treatment of dam security risks needs to cover such areas as security hardening, security hardware, access control and zoning, security surveillance and response measures.

It is impossible to prescribe the appropriateness of security measures generically for all dams as each dam is site specific and consideration of the environment, threats and risks at each dam will determine the most appropriate level and type of security measures required. In this regard, all or nothing access measures may be appropriate at dams or alternatives of restricting access after hours and allowing supervised access during working hours may be viable. In addition there is a range and various standards of physical barriers available to suit various detection and response times. The problem is in defining the circumstances and measures which are appropriate.

Overall dam security has to be balanced with effective dam operation and public access expectations taking into account consequences and vulnerability.

7. SECURITY OPERATION, MAINTENANCE AND REVIEW

7.1 O&M Manual

There is a need to carefully consider the amount of security information that is placed in the general O&M Manual for a dam. Some organisations may have a holistic security program which includes an overarching security strategy or plan and subordinate site plans. They may also have a set of security standards, guidelines or procedures. The extent of planning and documentation will be dependent on risk and the security requirements of the particular site and organisation. For those organisations without adequate internal expertise in security, the NSW Police should be consulted to determine the extent of security planning required given the risk involved. External consultants may need to be engaged.

The DSC considers that a dam's O&M Manual should have a separate section which records the importance of dam security, records clearly the responsibilities and accountabilities for security and identifies where the security plans, standards, assessments and procedures are for the dam site. Repeating security measures in the O&M Manual has security concerns and runs the risk of inconsistencies and confusion of which document has priority. There is also the risk that operators will only read the O&M Manual for their security guidance and then not bother to read the overarching or more holistic security documents.

7.2 Employee Requirements and Training

The DSC considers that dam owners should ensure that:

- There are clear responsibilities for security from the corporate level down to the individual;

- All employees are instructed that they have a responsibility for security and it should form part of their position descriptions and performance agreements; and
- All employees are appropriately trained in their security roles with regular updates.

It is important for dam owners to identify the need, and arrange, for their employees to undergo induction and ongoing awareness training on matters such as:

- The security threat and risks;
- Their organisation's security strategy or plans and their role in them;
- Security reporting (including reporting of security incidents) and the value of security related information; and
- What constitutes a security incident?

Dam owners should also have in place a guideline to the minimum / appropriate level of security vetting for personnel that have access to their dams. This may be scaled dependent on the type / size of dam, its failure consequences, criticality and vulnerability. Vetting may range from none to a police check, ASIO check, background verification check or professionally vetted to a prescribed level.

7.3 Testing

The DSC considers that dam owners should conduct regular security exercises at their dams involving all affected personnel. They should usually be carried out annually at Extreme Consequence Category dams ranging back to five yearly at Significant Consequence Category dams (see Table 2 for details).

The exercises should be relevant to the threats / risks at the dam or to test changes in security plans. Escalation and de-escalation of the security levels incorporated within plans should form part of any exercise. The emphasis of the testing regime should be to identify vulnerabilities and improve security, rather than to punish or embarrass areas that are not complying.

7.4 Review Requirements

The DSC considers that dam owners should have a corporate security strategy that includes requirements for:

- Periodic surveys that completely examine existing security arrangements and measures should be conducted to support security planning. Checking compliance with existing plans and standards should form part of these surveys. They should be undertaken by someone with a holistic understanding of security practices and sufficient expertise in security risk management to provide appropriate advice. They should occur at intervals determined by the owner but, where there are risks to community welfare or interests, at least at the frequency indicated in Table 2;
- Periodic internal security reviews should be ongoing within dam organisations through a corporate security committee or security manger / coordinator. Their purpose is to review particular parts of security. They may be initiated due to a change in threat or perceived ineffectiveness of a measure or at regular intervals

relating to the Consequence Category of the dam. The frequency is to be determined by the owner but, where there are risks to community welfare or interests, at least at the frequency indicated in Table 2; and

- Periodic internal security inspections that provide a focussed check that recommended / mandated security measures have been implemented and are working as anticipated / required.

Table 2 summarises these review arrangements with all security surveys, reviews and inspections to be appropriately documented (i.e. in-confidence internal documents) and reported to the Executive of the dam owner organisation with critical deficiencies reported to the DSC (see Section 5) and police etc if appropriate.

Table 2 - Dam Security Testing/Review Guidelines where there are Risks to Community Welfare or Interests

Requirement	Extreme Consequence Dam	High Consequence Dam	Significant Consequence Dam
Dam Security Desk-Top Exercise	Annually	Two-Yearly	Five-Yearly
Dam Security Field Exercise	Two-Yearly	Three-Yearly	Five-Yearly
Review of Site Security Plan	Annually	Two-Yearly	Five-Yearly
Focussed Security Inspections & Reviews	* As Required	* As Required	* As Required

(* As required to validate security measures that may be ineffective, or to randomly verify effectiveness, or to ensure new / modified measures are working as anticipated etc. - usually aligned with security exercises).

8. DOCUMENTATION

8.1 Minimum requirements of DSC

The DSC requires dam owners of Significant or higher Consequence Category dams to maintain the following security documentation:

- A risk-based security plan that addresses security arrangements for each dam (for larger organisations this may include both a strategic framework and a site specific plan);
- Current security threat, vulnerability and risk assessments for each dam (some of which may be supplied from external agencies);
- Procedures for reporting security information and responding to security incidents;
- Record of the outcomes of security surveys and reviews on each dam; and
- An O&M Manual for each dam which has a separate section referring to security responsibilities and identifying the location of the above documentation.

8.2 Sensitivity of information

The DSC considers that all information detailing security threats, risks, plans and measures should be categorised as STAFF or SECURITY-IN-CONFIDENCE at a minimum. *Each dam organisation must define in their information security strategy how they protect this information and who can have access.*

The Commonwealth Protective Security Manual is a good source of guidance on appropriate information security practices while *AS/NZS ISO/IEC 27001:2006 Information Technology – Security Techniques – Information Security Management Systems – Requirements* also outlines a detailed process for effective information security management which may be adapted for use by dam owners.

9. REFERENCES AND SOURCES

The following references and sources are presented to provide assistance to owners in consideration of a range of matters pertinent to dam security:

- ANCOLD (Australian National Committee on Large Dams), *Guidelines on Assessment of the Consequences of Dam Failure*, May 2000
- ANCOLD (Australian National Committee on Large Dams), *Guidelines on Dam Safety Management*, August 2003
- ANCOLD (Australian National Committee on Large Dams), *Guidelines on Risk Assessment*, October 2003
- AS/NZS ISO/IEC 27001:2006 *Information Technology – Security Techniques – Information Security Management Systems – Requirements*
- *Commonwealth Critical Infrastructure Protection Risk Management Framework for the Identification and Prioritisation of Critical Infrastructure*
- Grayman, Deiniger & Clark, *Keep it Safe* (see www.cenews.com)
- *Locking Down on System Security* (see www.americancityandcounty.com)
- National Crime Prevention Council, Singapore, *Crime Prevention through Environmental Design Guidebook*
- *NSW Critical Infrastructure Protection Management Framework,* February 2005
- Pritchard, S, *Stepping up Security* (see www.connectingpower.com)
- Risk Management Institute of Australasia*, Security Risk Management Body of Knowledge (SRMBOK), 2007*
- Sandia National Laboratories, *Risk Assessment Methodology for Dams (RAM-D*, Albuquerque, USA (see www.sandia.gov)
- Standards Australia/Standards New Zealand, *Information Security Management Part 2: Specification for Information Security Management Systems*, AS/NZS 7799.2:2003

- Standards Australia/Standards New Zealand, *Information Security Risk Management Guidelines, HB231:2004*
- Standards Australia/Standards New Zealand, *Risk Management*, AS/NZS 4360:2004
- Standards Australia/Standards New Zealand, *Security Risk Management Guidelines, HB167:2006*
- United States Federal Energy Regulatory Commission, *Dams Assessment Matrix for Security and Vulnerability Risk (DAMSVR)-Comprehensive Manual-Version 2, 5 June 2009* - (see http://www.ferc.gov/industries/hydropower/safety/security.asp).

This Guidance Sheet is one of a series available from our Website at:

http://www.damsafety.nsw.gov.au

In order to read this file you need a Portable Document Format (PDF) reader. A free PDF reader is available from http://www.adobe.com/

For any further information please contact:

NSW Dams Safety Committee
Level 3, Macquarie Tower
10 Valentine Avenue, Parramatta NSW 2150

PO Box 3720, Parramatta NSW 2124

☎ (02) 9842 8073 (02) 9842 8071

dsc@damsafety.nsw.gov.au

ISSN 1039-821X