JACOBS

Wagga Wagga - Stage 3

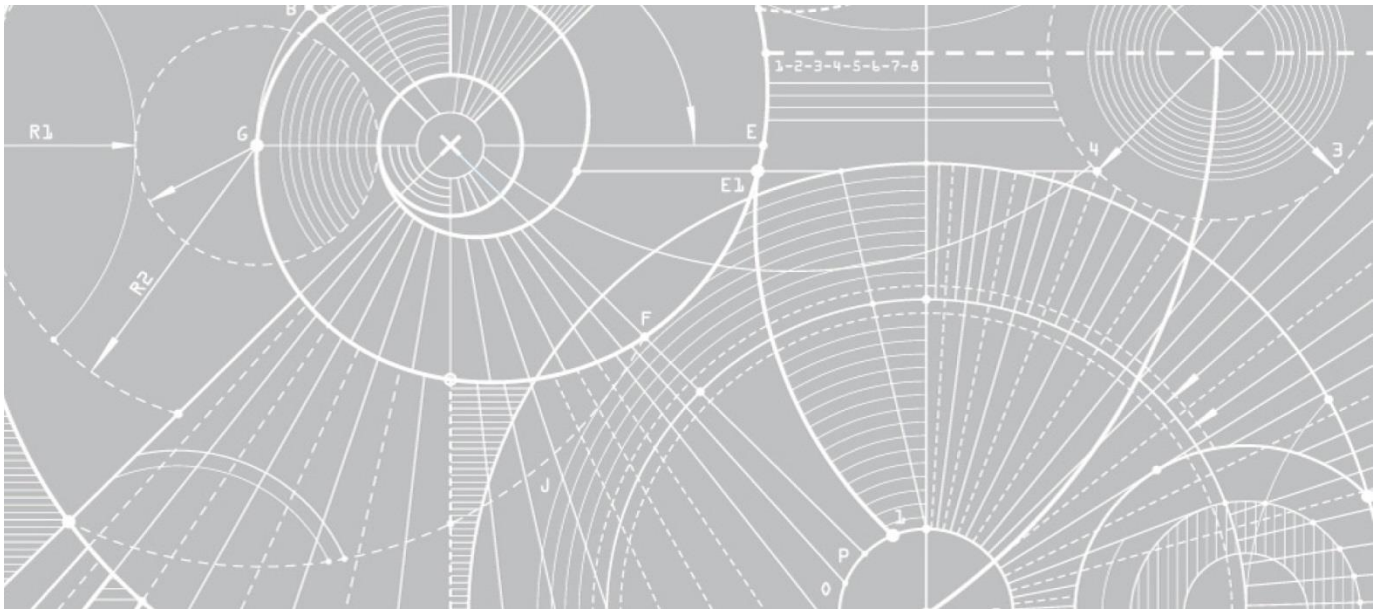
NSW Health Infrastructure

Security Risk Assessment

IA172200-MHI-SRA-0001 | B

05/03/2018

NSW GOVERNMENT | Health Infrastructure



Document History and Status

Wagga Wagga - Stage 3

Project No:	IA172200
Document Title:	Security Risk Assessment
Document No.:	IA172200-MHI-SRA-0001
Revision:	A
Date:	28/02/2018
Client Name:	NSW Health Infrastructure
Client No:	IA172200116500/300
Project Manager:	Mihaela Serban
Author:	Guy Clifford
File Name:	C:\Users\cliffog\Desktop\HOSPITAL\IA172200- Wagga Stage 3.docx

Jacobs Group (Australia) Pty Limited
ABN 37 001 024 095
Level 7, 177 Pacific Highway
North Sydney NSW 2060 Australia
PO Box 632 North Sydney
NSW 2059 Australia
T +61 2 9928 2100
F +61 2 9928 2500
www.jacobs.com

Revision	Date	Description	Author	Reviewer	Approver
A	28/02/18	Draft for Client Review	GC	PG	MS
B	05/03/18	Final Report	GC	PG	MS

`

Contents

List of Tables

1. Executive Summary

1.1 Executive Summary

The NSW Government (Health Infrastructure) has approved a redevelopment within the grounds of Wagga Wagga Rural Referral Hospital. This project (Stage 3) is to demolish an existing section of the Hospital on the north western sector of the site and construct a four (4) level building including a further plant room level (roof) and a basement (underground) carpark with 89 spaces.

The “Ambulatory Care” Building will house a number of public health services including;

- Elderly Care
- Breast Screening
- Renal & Oral Health Care
- Allied Health
- Ambulatory Rehabilitation
- Education, Library and Office spaces
- 24 Bed rehabilitation Inpatient Unit (linked to the existing Stage 2 ASB)

Jacobs has been engaged to provide expertise in Project Management, Project Controls, Procurement, Engineering and Construction including Electrical and Mechanical design.

To facilitate the Security design of the building, this Security Risk Assessment (SRA) has been undertaken to objectively assess the proposed building design with respect to known and or potential risks within the precinct. This SRA will also assist the Architects in the development of any design-related risk treatments that may be identified during the SRA. The scope of this document is to identify those vulnerabilities and security risks as they relate to the current redevelopment (Stage 3), however, consideration has been given to any identified issues from Stage 1 or 2 that may impact the Stage 3 design.

The risk mitigation strategies and treatments proposed in this assessment were developed in conjunction with the principles of NSW Heath Policy Guidelines for Security Risk Management in Health Facilities. The recommendations derived from the SRA may be used to assist the overall security design and surrounding environment.

1.2 Key Findings

Generally, the existing security controls within the Wagga Wagga RR Hospital were considered to be commensurate with good Security Industry practice. Wagga Wagga Local Government Area (LGA) is projecting a positive population trend in coming years, therefore it is reasonable to expect that as the local area and the outlying areas continue to expand, so will the threat context and the threats that pose a risk to Wagga Wagga RR Hospital.

Below is a summary of the identified key issues identified during the Assessment:

- Need to secure the basement carpark to a high level to ensure of safety and security for staff & visitors
- Access Control on basement carpark fire doors to supplement security and safety for staff & visitors
- Review report and resolve issues on existing CCTV system to eliminate potential on-going issues into Stage 3
- Review the need for CCTV coverage in existing at-grade carparks for issues of Safety & Security
- Review CCTV cameras resolution and recording configurations to enhance existing surveillance
- Review of Mobile Duress products with a view to product standardisation
- Review of monitoring capability of additional CCTV cameras and consider current security office configuration

Further information on these issues is contained in section 4.5 of this report.

1.3 Overview

Wagga Wagga Rural Referral (RR) Hospital is a major NSW Regional hospital located on the corner of Edward Street (Sturt Highway) and Docker Street in central Wagga Wagga. The hospital operates as a base public hospital for the population of approximately 65,000 residents and is the largest referral hospital in the Murrumbidgee Local Health District with an emergency Department seeing more than 40,000 patients per annum.

Figure 1 – Wagga Wagga Rural Referral Hospital Site

1.4 Hours of Operation

Wagga Wagga RR Hospital provides 24/7 healthcare services via the Emergency Department, however the primary hours of operation of the Hospital are from 0600 to 2000 hours each day. With the exception of the Emergency Department, all perimeter doors are closed at 2000 hours, with after-hours visitor access available via the Security Office located adjacent to the Emergency entry.

1.5 Vehicle and Pedestrian Movement

The main vehicle entry into the Hospital precinct, is directly off Edwards Street (Sturt Highway) into what was originally Lewis Drive (see Figure 2). There are additional vehicle entry points at the rear of the precinct but have only restricted access and parking see Figure 3). The majority of current staff and visitor parking space is located to the North of the precinct in proximity to the main entrance driveway.

Figure 2 – Wagga Wagga Main Vehicle Entry

Figure 3 – Rear Lane Access

2. Scope of Assessment

2.1 Scope of Assessment

The purpose of this SRA is to independently evaluate the security risks associated primarily with the design of the new Stage 3 works, however, to ensure continuity in design, risks or issues identified as generated from previous works, that may affect the design outcomes of the new building were also considered.

This SRA is the product of a site survey, reviews, consultation with external parties, and a meeting attended by Jacobs' Security Consultant. The meeting was also attended by Consultants from other disciplines, including Jacobs Electrical, Philip Chun (BCA), Martin & Ollman (Architects), Wagga Hospital Security Manager and Savills Project Management. In the preparation of this report, Jacobs has also considered possible external threat scenarios that could be directed at the Wagga Wagga RR Hospital precinct that may also inadvertently impact the design outcomes.

Jacobs' risks analysis also considered:

- Protecting People & Property – NSW Health Policy and Standards for Security Risk Management in NSW Health Agencies – June 2013
- Existing Security Systems that are to be expanded for Stage 3
- Crime Statistics provided by the Bureau of Crime Statistics and Research
- A review of the proposed and previous security design

Jacobs' assessment utilised the Crime Prevention Through Environmental Design Principles (CPTED) as well as our integrated approach to security. The security risk assessment involved a high level vulnerability or gap analysis of the proposed security controls, a high level qualitative analysis of local area crime statistics, geographical and operational threat profile analysis and the development of a qualitative security risk register.

This SRA did not consider information security (cyber security) within the scope of this report.

2.2 Security Risk Management Philosophy

There are no guarantees in the risk management process, and the prescribed treatments aim to reduce the likelihood and consequences from the identified risks.

It is acknowledged that to protect the organisation holistically and in a manner which would provide a guarantee against all risks would be impossible to achieve. In addition, the costs associated with implementing such a philosophy, and the controls that would be required to achieve a situation of no risk, would be unreasonable. Therefore, the risk responses and treatments are not designed to eliminate the risk, but rather reduce it to a point where it is "As Low as Reasonably Practicable" (ALARP) and can be effectively managed.

3. Risk Methodology

3.1 Methodology

The methodology used throughout the SRA is based on the *ISO 31000:2009 - Risk Management - Principles and Guidelines*, in conjunction with *HB 167:2006- Security Risk Management*. Our methodology applies these principles in conjunction with the *NSW Health Risk Management Framework - 2015*, and Jacobs unique and in depth understanding of the risk management process.

In consideration of this assessment, the following steps were taken:

- Concerns raised by key stakeholders
- Identification of credible risks and threats which are generic, site specific and perceived
- High level analysis of the local area
- Review of proposed site's existing security measures
- Determination of assets
- Review of existing security arrangements including physical, technological and management
- Determination of authorised and restricted pedestrian and vehicular movement across the sites

Our approach to this involved the following:

- A series of site surveys
- A meeting with relevant stakeholders
- Review of security concerns raised by staff and parents within an internal security review
- Review of all available documentation of site security related incidents
- Research of relevant industry and other Health policies, standards and guidelines
- Desktop review of the proposed building Design

3.2 Risk Profile Development Process

With consideration to the risk treatment principles of:

- Identify the risk
- Evaluate the risk
- Never accepting unnecessary risk
- Accept risk only when the treatment cost outweighs the benefits
- Where possible, risks should be managed at the point where they occur

The process Jacobs followed identifies risks and provides advice on the available controls to enable the design team, in consultation with stakeholders, to effectively reduce specific risks to an ALARP level. The process adopted includes:

- Identify what can happen
- Identify how it can happen
- Evaluate the likelihood of occurrence
- Evaluate the consequence of the occurrence
- Identify and evaluate the controls that can be applied
- Establishment of anticipated residual risks
- Provide guidance to continue the assessment process for periodic review

Additional components of the process are identified within flow chart below:

Figure 4 - Security Risk Management Process

3.3 Risk Identification

By establishing the context, the organisation articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process. While many of these parameters are similar to those considered in the design of the risk management framework (see 4.3.1), when establishing the context for the risk management process, they need to be considered in greater detail and particularly how they relate to the scope of the particular risk management process.

3.4 Risk Analysis

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analysed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

3.5 Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

3.6 Risk Treatment

The risk treatment process used involved a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options considered included the following:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Taking or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing); and
- Retaining the risk by informed decision.
- Risk Re-Evaluation

The purpose of risk re-evaluation is to analyse the effectiveness of any prescribed risk treatments.

3.7 Assessment Risk Matrices

Likelihood	Criteria
Almost certain	Will occur on an annual basis
Likely	Has occurred several times at similar facilities
Possible	Might occur once in the life of the facility
Unlikely	Occurs somewhere from time to time
Rare	Heard of this happening elsewhere
Very Rare	Never heard of this happening
Not expected to occur	Theoretically possible but unexpected

Table 1 - Security Risk Likelihood (adapted from HB 167:2006)

Consequence	Impact on Individual Safety / Centre Operations / Financial
Extreme	Catastrophic incident
Major	Serious incidents
Moderate	Major incident
Minor	Significant incident
Negligible	Insignificant safety incident

Table 2 - Security Risks Consequence (adapted from HB 167:2006)

		Consequence				
		Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
Likelihood	**Almost certain**	Very Low	Low	Moderate	High	Extreme
	Likely	Very Low	Low	Moderate	Moderate	Very High
	Possible	Very Low	Low	Low	Moderate	High
	Unlikely	Very Low	Very Low	Low	Moderate	Moderate
	Rare	Negligible	Very Low	Low	Low	Low
	Very Rare	Negligible	Very Low	Very Low	Very Low	Low
	Not expected to occur	Negligible	Negligible	Negligible	Very Low	Very Low

Table 3 - Risk rating matrix (adapted from HB 167:2006)

NSW Health Risk Matrix

Risk rating	Action required
Red = Extreme (A – E)	**Escalate to CE or Head of Health service or Secretary, MoH** A detailed action plan must be implemented to reduce risk rating with at least monthly monitoring and reporting.
Orange = High (F – K)	**Escalate to Senior Management** A detailed action plan must be implemented to reduce risk rating.
Yellow = Medium (L – T)	**Specify Management Accountability and Responsibility** Monitor trends and put in place improvement plans.
Green = Low (U – Y)	**Manage by routine procedures** Monitor trends.

NSW HEALTH RISK CATEGORIES	CONSEQUENCE EXAMPLES				
	Catastrophic	Major	Moderate	Minor	Minimal
Clinical Care & Patient Safety	Unexpected multiple patient deaths unrelated to the natural course of the illness.	Unexpected patient death or permanent loss/reduction of bodily function unrelated to the natural course of the illness.	Unexpected temporary reduction of patient's bodily function unrelated to the natural course of the illness which differs from the expected outcome.	Patient's care level has increased unrelated to the natural course of the illness.	First Aid provided to patient unrelated to the natural course of the illness.
Health of the Population	An increase in the prevalence of known conditions contributing to chronic diseases across the state-wide population health KPI categories currently measured by NSW Health and or an increase of more than 10% in one or more category.	Failure to materially reduce the prevalence of known conditions contributing to chronic disease across the majority of the state-wide population health KPI categories measured by NSW Health and or an increase of more than 5% up to 10% in one or more category.	Failure to materially reduce the prevalence of more than one of the known conditions contributing to chronic disease from the state-wide population KPI categories measured by NSW Health and or an increase of more than 2% and up to 5% in one or more category.	Failure to reduce the prevalence of one of the known conditions contributing to chronic disease from the state-wide population health KPI categories measured by NSW Health or an increase of up to 2% in one or more category.	A preventative Health program has not demonstrably met planned objectives but the prevalence of known condition is continuing to decrease in line with KPI targets.
Workforce	Unplanned cessation of a critical state-wide program or service or multiple programs and services.	Unplanned cessation of a service or program availability within a Service Area with possible flow on to other locations.	Unplanned restrictions to services and programs in multiple locations or a whole hospital or community service.	Unplanned service delivery or program delays localised to department or community service.	Minimal effect on service delivery.
Communication & Information Facilities & Assets Security	Cessation of services due to loss, damage or unauthorised access to property, assets, records and information.	Prolonged service disruption or suspension of services due to the loss, damage or unauthorised access to property, assets, records and information.	Temporary suspension of services due to the loss, damage or unauthorised access to property, assets, records and information.	Localised disruption to services. Minor loss, damage or unauthorised access to property, assets, records and information.	Minimal effect on services. No loss or damage to property, assets, records or information.
Emergency Management	State-wide system dysfunction resulting in total shutdown of service delivery or operations.	Services compromised as service providers are unable to provide effective support and other areas of NSW Health are known to be affected.	Disruption of a number of services within a location with possible flow on to other locations in the area.	Some disruption within a location but manageable by altering operational routine.	No interruption to services.
Legal	Legal judgement, claim, non compliance with legislation resulting in indeterminate or prolonged suspension of service delivery.	Legal judgement, claim, non compliance with legislation resulting in medium term suspension of service delivery.	Legal judgement, claim, non-compliance with legislation resulting in medium term but temporary suspension to services.	Legal judgement, claim, non-compliance with legislation resulting in short term disruption to services.	Legal judgement, claim or legislative change but no impact on service delivery.
Finance	More than 5% over budget NOT recoverable within the current or following financial year. Unable to pay staff or finance critical services.	Up to 5% over budget or a material overrun NOT recoverable within the current financial year. Unable to pay creditors within MOH benchmark.	Up to 5% over budget but recoverable within current financial year.	Up to 1% temporarily over budget and recoverable within current financial year	Less than 1% over budget. Temporary loss of or unplanned expenditure related to individual program or project but no net impact on budget.
Work Health & Safety	Multiple deaths or life threatening injuries or illness to non-patients.	Death or life threatening injury or illness causing hospitalisation of non-patients.	Serious harm, injury or illness causing hospitalisation or multiple medical treatment cases for non-patients.	Minor harm, injury or illness to a non-patient where treatment or First Aid is required.	Harm, injury or illness not requiring immediate medical treatment.
Environmental	Permanent effect on the environment or is unlikely to recover.	**Long term effect on the environment. The environment will only recover through external assistance / intervention (EPA)**	Short term effect on the environment. Environment likely to make a full recovery through local planning and response measures.	Minor effect on the environment. Environment to make a full recovery by routine procedures	No lasting effect on the environment.
Leadership and Management	Failure to meet critical priority KPI's included in the service's performance agreement. Sustained adverse national publicity. Significant loss of public confidence, loss of reputation and/or media interest across NSW in services.	Failure to meet a significant number of priority KPI's included in the service's performance agreement. Sustained adverse publicity at a state-wide level leading to the requirement for external intervention. Systemic and sustained loss of public support/opinion across a service.	Failure to meet a number of priority KPI's included in the services' performance agreement. Increasing and broadening adverse publicity at a local level, loss of consumer confidence, escalating patient/consumer complaints. Extended loss of public support/opinion for a Facility/Service.	Failure to meet one or more of the KPI's (excluding priority KPI's) included in the service's performance agreement. Periodic loss of public support.	Minimal impact on local operations, local management review and occasional adverse local publicity.
Community Expectations					

Probability	Frequency	LIKELIHOOD	CONSEQUENCE RATINGS				
			Catastrophic	Major	Moderate	Minor	Minimal
> 95% to 100%	Several times a week	Almost certain	A	D	J	P	S
> 70% to 95 %	Monthly or several times a year	Likely	B	E	K	Q	T
> 30% to 70%	Once every 1 -2 years	Possible	C	H	M	R	W
> 5% to 30%	Once every 2 – 5 years	Unlikely	F	I	N	U	X
< 5%	Greater than once every 5 years	Rare	G	L	O	V	Y

Table 3

Figure 5 - NSW Health Risk Management Matrix

JACOBS

4. Security Risk Assessment

4.1 Overview

The types of security risk events that affect the Hospital Precinct can be identified through an analysis and understanding of the strategic and operational threats that impact hospital environments.

It is important to acknowledge that the consequences and overall risk ratings were established with reference to the potential impact and effects on individuals who use the Hospital, and includes consequences to the overall infrastructure and assets.

4.2 Threat Sources

Generally speaking, security threats tend to be derived from human sources, rather than those arising from the natural environment. As such, and for the purposes of risk planning, it has been typical within hospital and the healthcare environment to categorise human-derived threats generally within the following groups:

- Drug, alcohol, and mental health affected person(s)
- Trusted Insiders (included former employees)
- Visitors and the Public
- Malicious Damage or Vandalism
- Theft (Staff & Visitor Property)
- Assault on Staff / Visitors or Patient
- Sexual Assault (Staff / Visitor / Patient)
- Criminals or Opportunists
- Wandering Patients
- Politically Motivated Groups
- Construction Activity
- Terrorists

There is however, an acknowledged limitation in the process of seeking to definitively categorise threat sources, as individuals and groups typically demonstrate characteristics of multiple types of threat. Examples may include a drug and alcohol incident that occurs at the Hospital that is related to a domestic dispute. Nonetheless, when risks derived from each group are considered holistically, this limitation tends to be largely mitigated.

4.3 Crime Profile

Criminal statistic data has been analysed and supported with information obtained from other sources and government agencies. The statistics used in this analysis were provided from the Bureau of Crime Statistics and Research (BOCSAR). The report captures recorded offences for the Wagga Wagga Local Government Area (LGA), not solely the Hospital precinct. Whilst this data has inherent limitations, it does capture the broader local geographical threats.

Offence	2015-2016	2016-2017	Trend
Theft	2817	2604	Decline
Malicious Property Damage	828	749	Decline
Assault	756	687	Decline
Harassment and Public Nuisance	378	319	Decline
Steal from Motor Vehicle	12	14	Stable
Sexual Offence	122	96	Decline
Drug Related Offences	498	427	Decline

Table 4 - Crime Statistics for Wagga Wagga LGA

4.4 Crime Data Analysis

Our analysis indicates higher than average levels of crime across the Wagga Wagga LGA due to the size of the region, in comparison to other key LGAs across NSW. Whilst the majority of offence appears to be in decline, the primary areas of concern are the number of Theft and Malicious Damage incidents, and the number of drug related offences over the period. In our assessment these trends are consistent with the broader Sydney metropolitan area and other Regional LGAs. It is also difficult to analyse what, if any, impact these trends will have on the Hospital precinct.

4.5 Identified issues Stage 3

4.5.1 Basement Car Park

The Stage 3 works includes an underground carpark providing approximately 89 spaces for Hospital Management, Staff and Ambulatory Care Patients. Any underground carpark generally creates additional risk to that of a street level at-grade carpark, due to the ability for criminals to conceal themselves in areas where they cannot be readily seen by approaching staff / visitors.

A review of the preliminary design of the underground carpark indicates that there may be a one (1) dual lane vehicle entry point off the existing at-grade carpark at the north-western end of the precinct. The carpark is serviced directly by the building elevators, which should negate the need for staff to use the emergency pedestrian exits on the north, south and western boundaries, as a normal path of egress.

To ensure that these fire exit doors are not used to gain access to the basement for the purposes of criminal activity they should be externally locked with card readers fitted only allowing authorised access into the carpark via the use of the Hospital Access Control system or the internal passenger lifts. This enhances the overall security of the carpark deterring potential offenders from gaining access to the basement carpark from those fire exit doors.

In designing the vehicular entry of the underground carpark, consideration should be given to the type of physical barriers to be installed. The installation of a boomgate on either side of the driveway entrance will provide controlled access by motor vehicles to the space, but will allow easy access for pedestrians.

The preferred option for the driveway entry would be to provide dual aluminium grill roller doors (see Figure 6), which would be managed through the use of the existing Hospital Access Control System.

This type of controlled entry door deters pedestrians from attempting entry as the portal is clearly designed for vehicle access. In addition to the aluminium grill roller door, the immediate area should be supplemented by the use of CCTV cameras to provide identification of any pedestrians attempting to gain access.

The use of two (2) individual gates ensures, that only the side with the waiting vehicle will open, which restricts any access by unauthorised vehicles or pedestrians to the opposing gate. If a single gate is used, both the entry and exit lanes are opened simultaneously providing an opportunity uncontrolled pedestrian access or egress.

Figure 6 - Example of Basement Carpark Security Roller

The second option is for a dual sliding gate at the entry to the carpark (see Figure 7).

Figure 7 - Example of Basement Carpark Dual Sliding Security Gates

The carpark should also have strategically placed CCTV cameras installed to provide surveillance capabilities for areas where natural surveillance is restricted, and for entry / exit portals and general traffic areas to enhance the overall security of the underground carpark.

The use of these types of gates as opposed to the use of boomgates strengthens the overall security of the underground carpark providing a safer environment for arriving and departing staff and authorised visitors and reduces the residual risk relating to issues of assault and theft from motor vehicles.

Number	Recommendation
1	Installation of access control readers externally on all carpark fire exit doors
2	Installation of a dual roller door or dual sliding gate to enhance security in the underground carpark
3	Installation of strategically placed CCTV cameras

4.5.2 CCTV System

During the site inspection it was noted that there were a number of CCTV system issues, where cameras were seen to intermittently drop offline and become unavailable. Those failing cameras ceased to provide data and therefore no images were recorded onto the system. The Hospital uses an Avigilon based software platform operating on Network Video recorders. The cameras types used throughout the Hospital are both Avigilon and Hikvision branded equipment. The regular camera failures are not restricted to either camera brand, with both products failing at any given time.

It was advised by Hospital Security that in November 2017, a full technical review and test of the existing CCTV system was carried out by a dedicated Avigilon technician with a report on the failing cameras due in February 2018. It is expected that this report will identify the cause of the on-going camera failures and a solution provided to ensure full functionality.

Given that the Stage 3 project will ultimately include a considerable number of new cameras introduced into the existing CCTV platform, it is critical that the cause of the failing cameras is identified and a solution implemented prior to commissioning of any new and or additional equipment.

It was identified that there was no CCTV coverage of the at-grade carparks within the precinct. The provision of CCTV within those spaces will provide the following benefits;

- Enhanced safety and security for staff transitioning from buildings to their vehicles after hours
- Ability to ensure that criminal acts (assaults/thefts) are pro-actively identified and addressed
- Additional coverage of Hospital grounds for the purposes of investigations and identification

It was noted during the inspection that there were a number of cameras where the images were of poor quality when digitally zoomed. This included both live and recorded images. The recorded images are likely as a result of the recording frame rates, which can be adjusted at the CCTV workstation and or server. Given that the images generated are 1080P, they should certainly be able to produce better and clearer vision. It is suggested that the camera configurations be interrogated by the security technicians and the cause of the poor images be corrected.

Number	Recommendation
4	Review CCTV report to ensure the identification and solution for the failing cameras is clearly defined prior to commissioning of additional equipment into the CCTV system
5	Review of CCTV coverage of at-grade carparks for enhanced coverage and safety of staff and visitors
6	Review of current cameras for image correction and configuration and review of system recording rates

4.5.3 Duress/Communication

The new Stage 3 project will require the installation of a duress and communications system. After reviewing the existing duress systems, it would appear that there are several different duress products operating throughout the Hospital including Ekotek, Ekahau and Spok. Experience has proven that the 'Ekahau' mobile product has the appropriate functionality and is preferred to other less flexible or proprietary products. Consideration should be given to standardising the duress equipment across the Hospital to ensure consistent operation and maintenance synergies.

There are fixed duress buttons located throughout the Hospital that are connected directly to the 'Gallagher' access control and intruder detection system and are considered fit for purpose and will be duplicated within the design of Stage 3.

Number	Recommendation
7	Review of Mobile Duress products with a view to product standardisation

4.5.4 Control / Security Room

The existing security office / control room, located inside the entry to the Emergency Department provides easy access for security personnel to the Emergency Department and also provides the ability to view incoming personnel and visitors to the ED.

Given that the construction of Stage 3 will likely increase the number of CCTV cameras across the network, this will likely increase the need for additional CCTV monitoring screens within the security room. During the inspection it was noted that the existing security room does not appear to meet ergonomic standards relating to the pro-active monitoring of multiple monitors, nor is the room ideal for installation of larger 55' monitors as there is insufficient depth, which does not allow the security staff to sit away from the monitors.

Should the Hospital wish to upgrade the monitoring capability of the security room, there would need to be a review and re-configuration both areas within that room to provide appropriate ergonomic resolutions and best practice design for security control rooms.

Number	Recommendation
8	Review of monitoring capability of additional CCTV cameras and consider current security office configuration.

4.5.5 Security Manpower

It should also be noted that on completion of Stage 3 there will be an extended requirement for security manpower services, for patrols, escorts, attendances to ever increasing aggressive behaviour and the monitoring of expanded systems.

To provide those expanded services including the pro-active monitoring of the CCTV system to an acceptable standard, may require additional manpower resources. The need for additional resources should be reviewed prior to completion of Stage 3 to ensure that appropriately trained personnel can be allocated to the expanded requirements.

Number	Recommendation
9	Review of manpower requirements to supplement expanding duties

4.6 Security Risk Register

Risk Category	Risk Event	Probability	Consequence	Risk Rating
Unauthorised Child removal	Unauthorised removal or abduction of a child from the Hospital	Possible	Major	Moderate
Trespassing	Unauthorised access to the facility's underground carpark areas	Almost Certain	Moderate	Moderate
Drug, alcohol and mental health affected person(s)	Harassing / Public Nuisance of staff and/or clients	Almost Certain	Moderate	Moderate
Trespassing	Unauthorised access to the facility's internal areas	Possible	Major	Moderate
Vandalism	Break windows with rocks, graffiti of facility surfaces, minor property damage	Likely	Minor	Low
Assault	Physical assault of a staff member or visitor in underground Carpark that causes an injury that requires medical attention	Likely	Major	Moderate
Assault	Verbal threats of aggression against staff due to dissatisfaction of service (over the counter) or domestic dispute	Likely	Moderate	Moderate
Theft	Theft of equipment from Hospital	Likely	Moderate	Moderate
Vehicle Accident	Accidental vehicle collision into a visitor staff member or Building Asset	Possible	Moderate	Low
Theft	Theft from vehicles parked in basement carpark	Almost Certain	Moderate	Moderate
Terrorism	Deliberate hostile attack on the facility or adjacent hospital facilities	Very Rare	Extreme	Low

Table 5 - Risk Register (Refer to Section 4.8 Risk Matrices)

4.7 Threat Sources

The following are designated potential sources of risk, or threat sources. When a threat source interacts with vulnerability, intentionally or non-intentionally, a risk is realised. The following list outlines potential threat sources to Wagga Wagga RR Hospital.

4.7.1 Drug and Mental Health Affected Patients/Visitors

Patients or visitors under the influence of drugs, excessive alcohol, or who suffer from mental health ailments can display anti-social behaviour including aggression and violent acts. As a source of threat within the hospital environment, it is not uncommon for staff to be verbally or physically abused.

Reports from Hospital Security, indicate there has been a considerable number of incidents where there was a need for physical restraint with patients, visitors, or the general public. It should be acknowledged that previous events with Methamphetamine affected patients (such as those at the Nepean Hospital 2016) have highlighted the unpredictable behaviour that can be experienced by Hospital staff. Due to the regularity of incidents, it can be expected that staff may be exposed to these situations.

4.7.2 Trusted Insider

Traditionally the trusted insider represents one of the greatest threats to an organisation. Trusted insiders are anyone who has access to an organisation's physical assets, facilities, funds and/or information including information technology systems. Trusted insiders can be past or present staff, visitors or contractors.

Due to their extent of knowledge and access, trusted insiders pose a threat to the organisation as they are well positioned to commit acts of theft, fraud, sabotage, and information disclosure.

4.7.3 Visitors and the Public

The majority of the public and visitors to the Hospital are generally considered to be low threat. This is because their presence within the Hospital's internal areas should be restricted to legitimate purposes only.

4.7.4 Malicious Damage or Vandalism

Malicious damage can result in minor issues such as graffiti or more severe issues such as disruption of services. Malicious damage can also create hazards which may create an unsafe environment for staff & visitors.

Sites that appear to be in a state of disrepair project a negative image to the public. This can decrease legitimate user perception of a safe, secure and controlled environment which is likely to decrease desirability of the area. Maintenance plans should be established to keep the external facets of the building in good repair.

4.7.5 Theft (Staff and Visitor Property)

The theft of staff or visitor property can occur from the external areas of the site, staff rooms, vehicles, etc. Theft of property can occur from one or a combination of threat sources. Generally, the theft of property can occur from any location and depends on the motivation of the threat source. For example, a criminal may enter the hospital precinct to steal building supplies from a construction area or specifically target staff or visitor personal property.

4.7.6 Theft of Prescription Drugs (Staff/Other Parties)

Prescription drugs are attractive items to many threat sources. As a Hospital, Wagga Wagga Hospital stores schedule 4 & 8 drugs in multiple locations throughout the precinct which are accessible to authorised personnel only. Threat sources may seek to exploit real or perceived vulnerabilities which can include physical and procedural controls to gain unauthorised access to the locations for the purposes of stealing drugs for personal use or for pecuniary gain.

4.7.7 Assault on Staff

An assault on Hospital staff or visitors can occur from a number of threat sources including other staff, parents and visitors, and a criminal act of aggression for the purpose of theft. The threat source, may suffer from mental illness or could be affected by drugs and alcohol. The Hospital Staff may also be inadvertently involved with domestic or custody disputes.

4.7.8 Sexual assault

Sexual assault on staff, patients and visitors can occur from any threat source. For the purposes of this security risk assessment report, sexual assault refers to incidents involving harassment, abuse (physical and verbal) or any other act that is considered to be of a sexual nature.

4.7.9 Criminals or Opportunists

Criminals and opportunists can either be legitimate users of the child care centre or visitors to the hospital precinct with the sole purpose of committing criminal acts. Crimes of opportunity can include breaking into vehicles or assaults in areas of the hospital precinct that are segregated with limited natural surveillance from passers-by.

4.7.10 Wandering Patients

Wandering patients are those patients that for whatever reason leave their ward without the knowledge of staff. This may be for reasons such as the patient is affected by drugs/alcohol, the patient is confused or suffers from mental illness or the patient is attempting to escape from local authorities. As a result, the patient could intentionally or unintentionally self-harm or harm other users of the Hospital.

4.7.11 Politically Motivated Groups

Politically Motivated Groups (PMGs) include extremist groups who may or may not rationalise the use of violence, or the threat of violence, as a means for promoting their rhetoric. PMGs can utilise a number of means to disrupt or degrade the primary objective of the Hospital. Hospital precincts, much like similar sized institutions such as universities, can be perceived by PMGs as places of mass gathering.

4.7.12 Major Construction Activities

Major construction activities include security risks associated with activities such as the redevelopment stages. This could include scenarios such as the theft of building equipment and materials or unauthorised access into building sites which could lead to harm.

4.7.13 Chemical, Biological, Radiological or Nuclear (CBRN) Event

Major events refer to those incidents where hospital staff may be exposed to the event through the course of their duties such as a Chemical, Biological, Radiological or Nuclear (CBRN) event.

4.8 Assets, Threat Sources and Security Risks

4.8.1 Primary Assets

Wagga Wagga RR Hospital is an essential Government asset. The ability for the Hospital to maintain health services in a safe, secure, convenient, friendly, and cost effective manner is an important consideration along with other important assets impacting the overall operation.

Based on this, the Hospital's primary assets are the people and the infrastructure;

People

- Patients
- Visitors
- Staff
- Contractors
- Service Providers

Property

- Medical Equipment
- Medical Facilities
- Education & Training Facilities
- Building Services (mechanical, electrical, communications etc.)
- Patient Property
- Staff Property
- Building Fabric and Fixtures

4.8.2 Secondary Assets

Reputation

- Wagga RR Hospital
- Murrumbidgee LHD
- NSW Health
- Local, State and Federal Government

Financial

- Operating Costs
- High value equipment
- Hospital Budget

Information

- Medical records
- Confidential Information
- ICT (Information Communication Technology) equipment such as computer and hard drives etc.

5. Risk Treatments

Risk Category	Risk Event	Probability	Consequence	Risk Rating	Recommended Treatments	Probability	Consequence	Residual Risk Rating
Unauthorised removal	Unauthorised removal or abduction of a child from the facility	Possible	Major	Moderate	• Hospital SOPs • CCTV • Electronic Access Control System • Duress Alarm System / Communications	Rare	Major	**Low**
Trespassing	Unauthorised access to the facility's underground carpark	Almost Certain	Moderate	Moderate	• Hospital SOPs • Automated Security Gates to Carpark • Electronic Access Control System • CCTV • Adequate Security Personnel	Possible	Moderate	**Low**
Drug, alcohol and mental health affected person(s)	Harassing / Public Nuisance of staff and/or clients while entering or exiting the Hospital	Almost Certain	Moderate	Moderate	• Hospital SOPs • Electronic Access Control System • CCTV • Duress Alarm System • Adequate Security Personnel	Possible	Moderate	**Low**
Trespassing	Unauthorised access to the Hospital's internal areas	Possible	Major	Moderate	• Staff SOPs • Electronic Access Control System • CCTV • Adequate Security Personnel	Unlikely	Moderate	**Low**
Vandalism	Break windows with rocks, graffiti of facility surfaces, minor property damage	Likely	Minor	Low	• CCTV • External Lighting • Maintenance Plan	Likely	Minor	**Low**

Risk Category	Risk Event	Probability	Consequence	Risk Rating	Recommended Treatments	Probability	Consequence	Residual Risk Rating
Assault	Physical assault of a staff member or visitor on site or in the underground carpark that causes an injury that requires medical attention	Likely	Major	Moderate	• Electronic Access Control System • CCTV in Carparks • Duress Alarm System • Staff SOPs • Automated Security Gates to Carpark	Unlikely	Moderate	**Low**
Assault	Verbal threats of aggression against staff due to dissatisfaction of service (over the counter) or domestic	Likely	Moderate	Moderate	• Staff SOPs • Electronic Access Control System • CCTV • Duress Alarm System • Adequate Security Personnel	Possible	Moderate	**Low**
Theft	Theft of Hospital equipment	Likely	Moderate	Moderate	• Electronic Access Control System • CCTV • Adequate Security Personnel • External Lighting	Likely	Minor	**Low**
Vehicle Accident	Accidental vehicle collision into a visitor staff member or Building Asset	Possible	Moderate	Low	• Physical barriers / Car park Design • Signage	Unlikely	Moderate	**Low**
Theft	Theft from vehicles parked on site and in underground carpark	Almost Certain	Moderate	Moderate	• CCTV • Automated Security Gate to Carpark • External Lighting • Adequate Security Personnel	Possible	Moderate	**Low**
Terrorism	Deliberate hostile attack on the facility or adjacent hospital facilities	Rare	Extreme	Low	• Electronic Access Control System • CCTV • External Lighting • Adequate Security Personnel	Very Rare	Extreme	**Very Low**

Table 6 - Residual Risk Table

5.1 Assessment Findings

The results of the assessment indicate that there are a number of risks rated at moderate, that with reasonable treatment would be reduced to a low risk. There are multiple threat sources that may be practically impossible to eliminate, but consequently, they tend to exist in most Hospital environments.

The most significant risks can be reduced by the strategic design of physical barriers and the appropriate use of CCTV and Access Control to eliminate unauthorised entry to areas where criminal activity would be more prominent.

5.2 Proposed Recommendations

Number	Recommendation
1	Installation of access control readers externally on all carpark fire exit doors
2	Installation of a dual roller door or dual sliding gate to enhance security in the underground carpark
3	Installation of strategically placed CCTV cameras
4	Review CCTV report to ensure the identification and solution for the failing cameras is clearly defined prior to commissioning of additional equipment into the CCTV system
5	Review of CCTV coverage of at-grade carparks for enhanced coverage and safety of staff and visitors
6	Review of current cameras for image correction and configuration and review of system recording rates
7	Review of Mobile Duress products with a view to product standardisation.
8	Review of monitoring capability of additional CCTV cameras and consider current security office configuration.
9	Review of manpower requirements to supplement expanding duties

Appendix A. CPTED

A.1.1 Crime Prevention through Environmental Design

The general CPTED principles that will apply to the Wagga Wagga RR Hospital are based on a number of concepts:

1) Natural Access Control
2) Natural Surveillance
3) Natural Territorial Reinforcement
4) Maintenance

These principles will be used within the concept and subsequent design stages to assist in reducing the dependency on security manpower and applied security technologies, both of which impose considerable ongoing costs.

The design of health care facilities needs to be conducive to a positive patient experience in order to achieve quality of life and efficient recovery. CPTED design philosophy encourages the design of a built environment that considers the nexus between aesthetics, functionality and the principles of security. Where possible the principles of CPTED should be applied and complemented by physical security controls, where appropriate, to provide an environment consistent with the context of health care.

A.1.2 Crime Prevention Theory

CPTED is a proactive approach to crime prevention, where the primary aim is to deter the likelihood of opportunistic crime occurring. CPTED uses passive techniques to achieve this and differs from the standard equipment based crime prevention techniques such as intruder alarms, CCTV, and Access Control and Intruder Detection (ACID) systems. However, it is recommended that CPTED and traditional target-hardening physical security measures be used together to achieve effective security solutions.

Three overlaying principles of CPTED can influence the way the physical environment is perceived by an individual. These are Territorial Reinforcement (TR), Natural Surveillance (NS) and Natural Access Control (NAC). All three principles should be taken into account when designing the structures for the Stage 3 works.

A.1.3 Natural Surveillance

Denying the ability for unauthorised persons to conceal themselves can present a higher perception of detection, and hence increase the apparent risk to an intruder. The increased apparent risk is an excellent crime deterrent which can be achieved by techniques to minimise the opportunity for intruders to conceal themselves and their actions. Well maintained landscaping with low shrubbery, uniform lighting and wide-open spaces will increase the natural surveillance features of the site. These crime prevention measures should be incorporated where possible into the building design and landscaping of the new Stage 3 building.

As an additional benefit, the effectiveness of electronic CCTV systems is further increased when NS techniques are employed, by providing clear sight lines.

A.1.4 Natural Access Control

Natural Access Control (NAC) prevents access to areas and creates a perception of detection and increased effort required by an offender with criminal intent. NAC is also used to regulate and channel pedestrian access into and out of a facility or site.

Lighting is a particularly effective technique to control the movement and concentrations of people. Individuals are attracted to brightly-lit areas at night and this can be employed to control pedestrian movements. Influencing the ways in which people gain access to a site provides greater control of the space by increasing the effort required by a potential offender to gain access to the space. Brightly lit areas can also be used to deter crime as there is a greater chance of being observed in a well-lit space. Specifically, providing additional lighting to the

building perimeter would be a useful crime prevention measure which would aid staff movements at night, deter trespassers and provide added lighting for CCTV coverage.

A.1.5 Territorial Reinforcement

Territorial reinforcement promotes social control through increased definition of space. An environment designed to clearly delineate private space does three things.

1) It creates a sense of ownership by the legitimate user.
2) The sense of owned space creates an environment where "strangers" or "intruders" stand out and are more easily identified.
3) By using buildings, pavement, signs, lighting and landscape to express ownership, natural territorial reinforcement occurs.

Territorial reinforcement measures make the authorised user feel safe making the potential offender aware of a substantial increased risk of apprehension or scrutiny.

JACOBS

JACOBS

www.jacobs.com | worldwide

Jacobs Group (Australia) Pty Limited
ABN 37 001 024 095
Level 7, 177 Pacific Highway
North Sydney NSW 2060 Australia
PO Box 632 North Sydney
NSW 2059 Australia
T +61 2 9928 2100
F +61 2 9928 2500
www.jacobs.com

October 26, 2016