Project Feasibility Analysis

Security Upgrade Program

Prepared for Ausgrid

January 2023

Table of Contents

1. Introduction & Background

1.1. Instructions & Scope

JLL has been engaged by Ausgrid to undertake analysis related to a selection of major property and some non-property projects. This analysis relates to the Security Upgrade Program (further details provided below in Section 1.3). This report provides indicative financial and non-financial observations relating the program.

1.2. Ausgrid Property & Accommodation Strategy

Ausgrid are continuing a program of consolidating and modernising their non-network property portfolio. The priority is to ensure they provide safe, secure and fit-for-purpose workplaces for staff that allows for the provision of timely and reliable services to meet customer needs. Further, there have been recognition of the need for better security management both internally within Ausgrid as well as through legislation (Security Legislation Amendment (Critical Infrastructure) Act 2021). Ausgrid is critical infrastructure and therefore need to ensure their depots and offices are secured for both operational requirements and for staff safety.

This Program seeks to target the main areas of security concern, including:

- Deny access to sensitive areas and equipment, especially given that high value equipment and material are stored at sites and are regularly targeted e.g., copper theft.
- Appropriate detection monitoring of office and depot accommodation.
- Prevent unauthorised access to sensitive information, with physical security being critical to ensuring cyber security.
- Depots are high industrial activity points and therefore restriction to access is required in order to enable safety for the general public).

Consequently, this program looks to address some of these concerns through the provision of:

- Access control
- Surveillance & monitoring
- Perimeter hardening & lighting

Ausgrid has identified the need for a number of projects involving the replacement, upgrading or refurbishment of property during the five-year forecast period. In particular, Ausgrid has an ageing property portfolio and priority has been given to those assets which are of greater safety and security concern and are in the most urgent need of replacement. A selection of these projects are the subject of the analysis we are now undertaking, as described in the instructions above.

1.3. Overview of the Proposed Projects

Ausgrid have developed a Security Upgrade Program which includes the following projects:

- Access control – upgrading building swipe access including capital hardware and equipment such as smart turnstiles to most modern integrated system. This will ensure; better tracking of entry and exit of persons into facilities, prevent access from unauthorised people and any breaches are recorded and to assist in prevention in the future.
- Surveillance & monitoring – continued rollout of detection cameras and infrared in logistics and depot facilities, which is transmitted back to a purpose-built security centre which monitors all facilities.
- Perimeter hardening & lighting – consistent fencing and lighting to prevent unauthorised access from deliberate attempts to access (e.g., criminal activity) and inadvertent access from children or other community members to ensure they do not access unauthorised areas, therefore avoiding safety risks.

2. Observations and Analysis

2.1. Drivers of Security Upgrade Program

Ausgrid recognised that historically the management of security had various issues including, being reactive rather than proactive, not consistent or streamlined. As such, Ausgrid began to prepare a Security Strategy which to provide a consistent risk management, that is both centralised and streamlined. In addition, Ausgrid's work on the Security Strategy began prior to:

- New legislation (Security Legislation Amendment (Critical Infrastructure) Act 2021) which requires greater security compliance. Adherence to this act will have impacts to the system and capital infrastructure required that will have to put in place. Ausgrid will need to adhere to these new security compliance measures to meet their legislative requirements.
- Some major and well publicised data breaches including Optus, Medibank and Telstra. The result of which led to private and personal sensitive customer information being published. It is yet to be understood what the long-term impact of these breaches will be but there is likely to be significant cost associated with rectifying these breaches, as well as personal cost to customers (which will likely be difficult to quantify). In addition, this has severely impacted the customer confidence in these organisations. These events further emphasise the importance of security, particularly cyber security.

Further to the above, some of the overarching key Ausgrid drivers for the proposed Security Upgrade Project include:

- Dynamic threat environment: Given the criticality of the infrastructure Ausgrid operates, the threat landscape is influenced by local and global issues which influence a threat actor's motivation to do harm. The Security Upgrade Program, as part of the broader Protective Security and Critical Infrastructure Strategy, addresses the need to improve the risk management capabilities in order to strengthen security controls in response to threats.
- Regulatory landscape: Reflecting the changing threat environment, the Commonwealth Government is declaring Ausgrid's network a "System of National Significance" under the Security of Critical Infrastructure (SoCI) Act. This declaration requires Ausgrid meet risk management practices and implement robust security controls that reflect the security threat and risk context.
- Technology evolution: Electronic detection and monitoring technologies continue to evolve through adoption of Artificial Intelligence and Automation. This presents an opportunity for Ausgrid to modernise their security controls to enhance their security detection and monitoring capabilities which enable improved incident response and can limit the consequence of security incidents.

2.2. Benefits of Security Upgrade Program

There are various benefits resulting from the Security Upgrade Program, some of these include:

- Security Governance: Ensuring Ausgrid's security is effective and complies with regulatory obligations.
- Personnel Security: People, resources and operations are protected from persons intent on harming Ausgrid.
- Physical Security: Protect against security threats by controls that are effective, efficient, standardised and respond to their risk context.
- Monitoring and Response: Effective capabilities that verify security incidents and mobilise timely and proportionate responses in order to reduce their impact.
- Security Risk Management: Ensuring decisions are proactive and focused on reducing the likelihood and consequences of negative events and exploiting opportunities.
- Security Culture and Awareness: All of Ausgrid contributes to the protection of Ausgrid's people and resources and the Security Upgrade Program will contribute through accommodating additional training and enhanced communications.

As seen from above, various benefits exist, however, many of these benefits are difficult to quantify or unable to be quantified but are still required (for example meeting the legislative requirement as outlined above). We have considered some analysis undertaken by Ausgrid which did attempt to quantify some of the benefits, where possible, which we have summarised below.

Reduction in Break-ins

Over the five years to 2022, ~$1.5 million worth of material has been stolen from non-network properties. Consequently, there are also investigation, repair and productivity loss costs. Based five-year averages, break-in and thefts cost $364,000 per annum. With the proposed capex program, a conservative theft reduction of 60% has been assumed due to improved security systems and physical barriers to premises, resulting in an annual benefit of ~$218,000.

Surveillance

Non-network security surveillance costs (for Ausgrid and external resources) are $168,000 per annum (five-year average). With an assumed reduction of 60% (as a result of improved CCTV and security systems), this represents a surveillance benefit of ~$101,000 per annum.

Cyber Risk

According to Ausgrid's cyber security team, the total cost of cyber threat consequences equates to ~$39.6 million (real FY24). As a conservative assumption, an anticipated reduction of 5% in cyber threats due to the 2024-29 capex program has been adopted, driven by increased security/surveillance and newer facilities that are less vulnerable and accessible. The cyber risk reduction benefit of the non-network property capex program (based on the 5% reduction factor) equates to ~$2.0 million per annum.

The above reflects a quantified benefit of ~$11.6 million over the FY25 to FY29 period, although we understand some of these annual benefits will continue beyond this regulatory period.

2.3. Key Observations

Provided earlier in this report, we have detailed the background, various drivers and benefits of the Security Upgrade Program. We understand the funds associated with Security Upgrade Program will help to deliver the Security Strategy being put forward by Ausgrid. A consistent risk management, that is also centralised and streamlined is important for many organisations, particularly one such as Ausgrid. This is further emphasised given the legislative changes that have come into effect (which recognise the importance), as well as recent cyber events.

Further, in addition to all the non-financial justification of the Program, Ausgrid have undertaken analysis to quantify some of the benefits, which equates to [redacted] over the FY25 to FY29 period or almost [redacted].

Disclaimer

The material contained in this report is confidential and was provided by JLL to the party to whom it is addressed strictly for the specific purpose to which it refers and no responsibility is accepted to any third party.

Neither JLL nor any of its associates have any other interests (whether pecuniary or not and whether direct or indirect) or any association or relationships with any of its associates that might reasonably be expected to be or have been capable of influencing JLL in providing this report.

Neither the whole of the report nor any part or reference thereto may be published in any document, statement or circular or in any communication with third parties or distributed without JLL's prior written approval.

Whilst the material contained in the report has been prepared in good faith and with due care by JLL, no representations or warranties are made (express or implied) as to the accuracy of the whole or any part of the report.

JLL, its officers, employees, subcontractors and agents shall not be liable (except to the extent that liability under statute or by operation of law cannot be excluded) for any loss, liability, damages or expense suffered by any party resulting from their use of this report.

If a projection has been made in respect of future demand, business trends, property prices, rentals and projected take up rates, such a projection is an estimate only and represents only one possible result therefore should at best be regarded as an indicative assessment of possibilities rather than absolute certainties. The process of making forward projections of such key elements involves assumptions about a considerable number of variables that are acutely sensitive to changing conditions and variations, and any one of which may significantly affect the resulting projections. This must be kept in mind whenever such projections are considered.

JLL is not operating under an Australian Financial Services Licence. The financial analysis and conclusions contained within this report do not purport to represent a valuation in the conventional sense. It is an exercise involving only relatively few variables, such as zoning information and a general knowledge of background market conditions; whereas, a valuation involves a detailed investigation of the property including, where appropriate, the nature of the locality, surrounding properties, full inspection, site peculiarities, the nature, quality and condition of improvements, comparable sales, market trends, yields, competition, design and layout and so on. The market value could be greatly affected by such factors, and by encumbrances, restrictions, or other impediments on Title which have not been considered in this report. Accordingly, the financial analysis contained herein is indicative only and not authoritative. It is merely a precursor to a formal valuation and should not be taken as a substitute for it.