RFP ID and Name	*RFP 3557 Security Systems Replacement Program*
Addenda No.	5
Relevant Section	Part B- Section 3 "Definition of the security systems"
Subject	Integration architecture and standards
Context	The additional information provided in this addendum about the nature of the integration of the five security systems will help Respondents scope and price their solutions more accurately. Please see below 'Attachment 14'.

Attachment 14. Integration architecture and standards

This section provides more information about the systems integration for the five security systems. It clarifies and supplements the information provided in Part B Section 3 (which should be read prior to reading this addendum) but does not replace it.

Sydney Airport is deliberately not being too prescriptive about the integration between the five security systems, since this will largely be defined by the products proposed by Respondents, the integration options provided by those products, and the ways that Respondents (and others) have implemented integration between those products before.

Integration between the five security systems and other Sydney Airport systems may require the systems to use specific mechanisms and protocols as supported by those systems and in-line with Sydney Airport standards and practices.

Sydney Airport's preference is for standards based integration to allow for greater interoperability between products, for example appropriate recognised industry standards such as ONVIF and OPC (especially the more loosely coupled OPC UA standard).

Sydney Airport recognises that product integration in the physical security domain is often by custom adaptors built using the target system's software development toolkit (SDK). Where there is no suitable standards based integration, proprietary product interfaces or APIs are acceptable provided that they are well documented, are widely accessible (to systems integrators and other software vendors) and will continue to be supported in the future.

Where custom integration is required, products should have supported capability for standard integration mechanisms (such as SOAP, XML, web services, RESTful APIs, IBM MQSeries).

Tight coupling between the five security systems, and between them and other systems, is to be avoided. Tight coupling is caused using mechanisms such as database sharing, use of unpublished or unsupported interfaces, or the direct use of devices (such as access controllers) by multiple systems.

There is a preference for intermediation of integration by the Enterprise Service Bus (ESB). Numerous integrations have been implemented at Sydney Airport. Patterns include request / response and publish and subscribe and HTTP and IBM MQSeries messaging are used as appropriate.

Configuration or development within the external systems to enable integration (including in the Sydney Airport ESB system where appropriate) will be performed by Sydney Airport and / or the parties that are responsible for those systems. Implementers of the five security systems will be responsible for the configuration or development for integration within the security systems they are implementing and the definition of suitable interface specifications.

The individual integration points with other systems identified within the RFP document are discussed in the following table. Respondents should develop plans and costs based on the initial integration expected and (where relevant) indicate in their solution description how the future integration might be achieved.

System	Integration with	Comments
Identity Management	Enterprise Document Management (EDM)	EDM is implemented using OpenText. It is expected that integration will be performed using OpenText's Content Management Integration Services (CMIS) interfaces
Identity Management	Finance system	Integration with finance systems (Oracle) will be by production of suitable structured documents for subsequent manual or automated upload
Identity Management	AusCheck	This will initially be an extract and upload / download process as supported by AusCheck today. Integration is by production and consumption of suitable CSV files (see Appendix E to Part B of the RFP) with the actual file exchange with AusCheck being a manual step. It is expected that callable services may be offered by AusCheck in the future and the use of these by the application would be preferred
Identity Management	Email	This will be by integration with the Sydney Airport Microsoft Exchange email system by means of SMTP

Identity Management	Training and certification systems	These systems are not currently automated to the point where they can submit or supply information electronically. It is expected that this data is captured manually by data entry (by ID administration users), as well as the ability to scan and load relevant documents
Identity Management	Security awareness test	This system currently produces a printed page of test results. It is expected that this practice will continue in the new system, with key data captured manually by data entry (by ID administration users), who will also scan and load the results sheet. Automated integration between the systems may be implemented in the future
Access management	Key Safes	Integration is primarily for adding and removing access to key safes for individual card holders. The Morse product (see Part B Appendix A) provides an API. Sydney Airport has the Illuminated LCD models and KeyPlusPro software (v2.0.4)
Access management	Legacy SACS	Integration is primarily for adding and removing access for individual card holders. The integration protocol used may differ for each system, due to the capabilities of the software for each system. ● The “Ground power and pre-conditioned air” system uses Honeywell EBI. OPC integration is expected ● The “Perimeter fence” system (currently being implemented) uses Gallagher Command Centre. OPC integration is expected ● “Car parking” uses PM Abacus. A custom web service integration is expected
Command and Control	Legacy SACS	This integration is the same as with Security Access Control (see Part B 3.16). Initially only the “Perimeter fence” system will be integrated and it is expected that this will use OPC.
Command and Control	Airport Operations System (AOS)	To obtain the details of an aircraft currently parked at a given bay (to support the pilot intercom function). This will be a simple RESTful web service call.

Command and Control	Voice and radio	Initially it is not expected that there will be programmatic integration with the voice system (currently Zetron AcomEVO). The locally installed client application window will be presented to users in a coherent screen layout in conjunction with other windows presented by the Command and Control system. Future capability might include the ability to make calls as an automated step in a workflow, or to launch a specific workflow in response to an incoming call
Command and Control	Monitor wall	Display to monitor wall solutions will be video output from operator workstations or by Command and Control client software running on workstations dedicated to the monitor wall, with the monitor wall controllers being external to the Command and Control software itself
Command and Control	Incident management	Initially it is not expected that there will be programmatic integration with the Incident Management system (Noggin OCA). The Noggin OCA web browser will be presented to users in a coherent screen layout in conjunction with other windows presented by the Command and Control system. The Noggin OCA web browser may be launched using a simple URL. Most security operations activities will not require the use of Noggin OCA
Command and Control	Video analysis tools	There is only one analytics system currently in place (the RESA tunnel system). It is expected that this (and future) analytics systems may generate alarms to be handled and also that the user interfaces for these systems can be launched and used in a coherent screen layout in conjunction with other windows presented by the Command and Control system.
Command and Control	Surveillance tools (e.g. perimeter radar)	Initially only the Honeywell RVS system will generate alarms upon intrusions being detected. Other systems may be implemented in the future

Command and Control	Electric fence	This system is the “legacy SACS” system listed as “Perimeter fence”, above
Command and Control	Duress alarms	Initially it is expected that the duress alarms will continue be connected to controllers within the Security Access Control system, which will generate alarms, and so no specific integration is expected. In the future duress alarm solutions may raise alarms directly
Command and Control	Fire	Initially it is not expected that there will be integration with the fire systems
Command and Control	Intercom	These devices will send an alarm to indicate that the intercom button has been pressed
CCTV	Monitor wall	Display to monitor wall solutions will be video output from operator workstations or by CCTV client software running on workstations dedicated to the monitor wall, with the monitor wall controllers being external to the CCTV software itself
CCTV	Video analysis tools	There is only one analytics system currently in place (the RESA tunnel system). It is expected that this (and future) analytics systems will be clients to the CCTV system, making use of high level interfaces to the CCTV server software rather than direct connection to cameras.