Department of Communications and the Arts

Feedback: Enterprise Security Strategy

Recommendations	Review feedback (Areas where document does not appear to meet requirements of the review)	Guidance / questions (Dept welcomes views on identified issues)	General Observations / Context	auDA response
Rec 24: As part of its international engagement (Recommendations 21, 22 and 23), auDA engage with key international security fora including ICANN's Security and Stability Advisory Committee to ensure that it is kept updated on international security developments. **Rec 25:** That auDA develop and implements an enterprise security strategy based on domestic and international best practice in consultation with all relevant stakeholders. **Rec 26:** That auDA publishes a public facing version of its enterprise security strategy, having regard to relevant sensitivities. **Rec 27:** As part of its stakeholder engagement plan (Recommendation 18), that auDA maps its relationship with Australian Government security agencies and the internet industry and community on security of the .au namespace. **Rec 29:** As part of its quarterly reports to Government (Recommendation 16) that auDA report on its security activities.	• The Critical Infrastructure Centre (CIC) noted it may be prudent that an IT security architect or other relevant cyber expertise be contracted to verify/audit and test the appropriateness of the Enterprise Security Strategy and the detail behind it. • The .au Review requires that auDA create an enterprise security strategy and a public facing version of the strategy. It is not clear if there will be separate versions? Noting comments from the CIC, the Department would recommend the development of a more detailed plan in line with Rec 25. • The CIC noted that the document talks about best practice without actually identifying what best practice is. The document should clearly state what best practice is and outline a pathway to achieving this.	• The Strategy focuses on technical security, but lacks detail around physical and personnel security (i.e. no information on how auDA will manage insider threat, build a security culture within the organisation, secure their physical premises etc.). CIC noted this same concern. • The CIC noted there is an overall lack of detail about how certain deliverables would be achieved and suggested cross-referencing with the recommendations from the Burgess Review auDA commissioned last year.	• Section 4 of auDA's Strategy states that auDA will seek the Australian Signals Directorate's (ASD) guidance on choices of hardware and software that meet ASD security standards. ASD has advised that while it encourages auDA to seek its advice, its guidance is typically to encourage organisations to conduct a best effort risk assessment.	• auDA has engaged an IT security architect from Security Shift Pty Ltd to review the Enterprise Security Plan and assist in developing an Information Security Management System (ISMS) to comply with ISO 27001. auDA will be engaging a separate firm to audit and certify auDA compliance with ISO 27001 (e.g. SAI Global). Our general approach with security is to meet documented best international practice and engage respected external auditors to confirm that this standard has been reached. • auDA does not intend to develop a different "strategy" for internal use. A strategy is by its nature a high-level plan with objectives, which auDA is happy to share publicly. auDA will as part of its corporate governance, produce annual operating plans including plans for security initiatives, and auDA will provide regular reporting of its delivery against the security strategy to both the Board and the Board's security and risk committee. High level updates will also be provided to, and feedback sought from, auDA's new Technical Advisory Standing Committee on an ongoing basis. • auDA does however create very detailed documentation as part of its development of a full suite of materials to meet the ISO 27001 standard, and other standards such as ISO 31000 (risk management), and ISO 22301 (business continuity). As this material is developed and approved, auDA is willing to share the detailed documentation with CIC under appropriate confidential agreements. • auDA is defining best practice as against international standards. auDA has specified the relevant international standards in the security strategy. The best practice is set out in those standards, which are publicly available. auDA will ensure that compliance with those standards is independently audited. auDA internally has an international expert in registry and registrar systems – Dr Bruce Tonkin was Chief Technology Officer of Melbourne IT, one of the 5 largest registrars globally for 18 years, and was a founding member of ICANN's security and stability committee and was the inaugural chair of the ICANN Board risk committee during the 9 years he was on the ICANN Board. • auDA is also engaging experts such as Chris Wright (Security Shift Pty Ltd) who was the Chief Technology Officer for AusRegistry, as well as Chief Security Officer (AsiaPac) for Neustar one of the top 3 registry operators in the world. auDA also works closely with Ram Mohan (Afilias) who is a current member of ICANN's Security and Risk Committee, and the Chief Technology Officer of Afilias (one of the top 3 registry operators globally). auDA's approach to best practice is determined by a combination of leveraging best practice material included in international standards, as well as leveraging the best practice experience of three internationally recognised experts.
