Contribution ID: **450** Type: **Paper**

Computer Security Considerations for Nuclear Material Software Development

This paper aims to illustrate how modern information security and best practice software development methodologies are applied to ensure appropriate information protection when storing or processing nuclear material inventory data. The Australian Government maintains a maturity based computer security framework for protecting digital systems and associated information. This is the basis for evaluating products, including web based software solutions, to ensure they are certified and accredited as capable of storing official information. Adapting the framework to ensure considerations for nuclear material information security include design, implementation and ongoing risk management activities that will be discussed in this paper. Industry standard software development methods ensure outcomes accurately achieve objectives, those being customer needs, security objectives, legal and compliance requirements, amongst others. Integrating computer security controls into the software development lifecycle ensures risk remediation occurs throughout each stage, and stakeholders understand and have visibility into the levels of risk present when developing and operating a web-based application containing nuclear material inventory data.

In order to successfully address each of these factors and incorporate them into a cohesive process, a hybrid software development lifecycle was adopted. A classic approach was utilised at the beginning and end of each project phase to ensure project governance requirements were satisfied. A design review was also performed at this stage in order to ensure both the stakeholders and project team were in agreeance on the deliverable for this phase. The classic methodology was combined with scrum and developer sprints. This was done not only to incorporate stakeholder engagement and feedback, but also guarantee that the outcome for each phase of the project was fit for purpose. Due to this high level of stakeholder engagement, all parties including security, regulators, the legal team and the client were able to ensure that their domain specific requirements were met. This paper will also outline other areas of the development practice, the technical framework used and illustrate how the continuous testing regime was instrumental in the successful delivery of the solution.

Gender

Male

State

Australia

Authors: STEVENS, Chris (Mr); Mr BARRY, Adam

Presenters: STEVENS, Chris (Mr); Mr BARRY, Adam

Track Classification: CC: Information and computer security considerations for nuclear security