Contribution ID: **549** Type: **Paper**

Providing Guidance for Creating Information Security Continuous Monitoring Programs to Support Transitioning to Ongoing Authorizations in Nuclear Security Programs

Historically, compliance-oriented computer security programs were built with a 'set it and forget it'mentality when it came to security control implementation in computing environments. Typically, the security control implementation would be revisited on a set multi-year recurring basis (e.g. every three years) where the security program would reevaluate the effectiveness of the security controls, make necessary security changes for the current operating environment, and seek reaccreditation from the Authorizing Official. This compliance-based approach to computer security is no longer considered an effective means of managing the security of todays computing environments. Compliance-based programs are not adequate to show current system risks and fail to help provide mitigations to combat modern threats.

Computer security standards bodies have encouraged security programs for years to move to ongoing authorizations that do not have a set date for reaccreditation. The continuous accreditation of the system relies on enhanced, near real-time information about the current security health given the organizations understanding of current threats coupled with current mitigations. Moving to an ongoing authorization strategy is dependent on the establishment of an Information Security Continuous Monitoring (ISCM) program. ISCM programs establish key metrics the organization monitors and provides information which helps govern the overall security health of the computing environment. They create threshold triggers which are set to ensure corrective actions are taken if the metric points move outside the desired threshold bounds. In some instances, the metrics provide information which help lead to quick response when real security incidents occur.

Incorporating an ISCM program helps move organizational computer security programs from sluggish, compliance-based programs to agile, risk-based programs that can quickly adjust to the ever-changing threats of today's computing environments. Nuclear regimes can enhance their ability to identify new threats and maintain current mitigations by adopting an ISCM program. ISCM program effectiveness has been vetted through years of use by various industries and when used appropriately by nuclear regimes, it will increase the efficiency with which nuclear security programs operate and provide better security for the industry as a whole. The paper would provide guidance specific to nuclear regimes on how to implement an ISCM program including relevant key metrics to monitor nuclear security systems which includes monitoring and assessment frequencies. The paper will also advise how the information from the selected metrics can be used to make rapid risk-based security decisions and how to assess your ISCM program to ensure the organization continues to track the relevant data to properly respond to emerging threats.

Gender

State

United States

Author: CHRISTENSEN, Drew (Pacific Northwest National Laboratory)

Co-author: CRAMER, Steven (Pacific Northwest National Laboratory)

Presenter: CHRISTENSEN, Drew (Pacific Northwest National Laboratory)

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