U.S. Air Force
Scientific Advisory Board

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE
WASHINGTON DC

Nuclear Surety and Certification for Emerging Systems (NCE)

Abstract

Certification is the final step needed to achieve the Initial Operational Capability (IOC) of a Nuclear Weapon System (NWS) and represents a key element of deterrence. The USAF nuclear enterprise has not certified a new platform since the B-2 in the early to mid-1990s. The adversary has advanced its capabilities to threaten nuclear weapon systems including cyber and supply chain attacks. The modernization program needs to respond to these threats. In addition to external threats, the next generation of weapon systems have grown in complexity both from software size and more complex hardware implementations to support flexibility and the potential for software feature updates, increasing the weapon attack surface.

The USAF Scientific Advisory Board (SAB) was tasked to conduct a study on "Nuclear Surety and Certification for Emerging Systems" in order to provide not only technological improvements to but ensure that the certification tasks are properly resourced with the right skills and priority. The NCE Study Panel distilled its findings into several recommendations based on rigorous examination of evidence gleaned from multiple briefings and discussions with the USAF and other organizations responsible for certification of critical systems. These recommendations include:

- The USAF should address the difference between the SAB resource estimates for the Air Force Nuclear Weapons Center (AFNWC), the Air Force Safety Center (AFSEC), and NWS Program Offices to support modernization
- An increased emphasis on the *Reliability* element of Surety is needed to address the evolving threat to USAF nuclear mission
- Develop and update instructions, policies, and procedures to address continual full-spectrum cyber resilience. Developing a cyber-resilient exemplar system should be considered. Elements could include: government off-the shelf (GOTS)-based reference architectures as trusted computing bases, tools to assess/mitigate supply chain risk, and formal methods to ensure secure software.
- In partnership with the NSA, develop a calculus for cyber resiliency (e.g., quantitative methods to measure mission impact). An equivalent to physical systems, where margins and uncertainties are analyzed and summed to give an indication of system reliability, should be developed in cyber space. Such a quantitative method would help prioritize cyber resources.
- Introduce additional system engineering processes at key points in nuclear weapons system certification. Migrating from pass-fail certification process to risk-based framework is needed to create a quantitative certification process that will reveal system impacts to technical trades.
- Add modernization certification status to Nuclear Oversight Board (NOB) meeting agendas to ensuring timely issue resolution, status could include manpower, resources, schedule, and challenges.

SAF-PA Approval: 2017-0366