Contribution ID: **587** Type: **Paper**

# The Need for Creative and Effective Nuclear Security Vulnerability Assessment and Testing

Realistic, creative vulnerability assessment and testing is critical to finding and fixing nuclear security weaknesses and avoiding over-confidence. In the U.S. experience, nuclear security systems that looked great on paper have often failed, in evaluations or tests, to protect against mock adversaries who had found a clever approach to defeating the defenders.

Both vulnerability assessment and realistic testing are needed to ensure that nuclear security systems are providing the level of protection required. A checklist approach that simply asks whether the system has all the particular elements required by regulations is not sufficient. Instead, systems must be challenged by experts thinking like adversaries, trying to find ways to overcome them.

Vulnerability assessment can make use of a variety of tools and approaches, from examination of individual security elements to find ways they might be defeated to complex computer simulation software modeling possible adversary efforts to defeat the system. Perhaps the most important element is the creativity and adversary mindset of the assessors; they should be genuinely looking for weak points, not just seeing whether the system will protect against a few pre-programmed attack strategies.

Nuclear security testing is closely related. Testing can provide data for use in vulnerability assessments and can help check the validity of assumptions and plausibility of proposed tactics. The results of realistic testing are often more convincing to organizational leaders and policymakers than any amount of paper or computer analysis. Testing can range from testing the performance of particular pieces of equipment to testing of the site's full security system in a force-on-force exercise. Here, too, it is key to ensure that testers are creative and thinking like adversaries, imagining and testing clever ways adversaries might attempt to defeat the security system.

Both effective vulnerability assessment and realistic testing are more difficult in the case of insider threats. Much of the software that has been developed for vulnerability assessment simulation is stronger for outsider threats than for insider threats, and finding realistic ways to test insiders' ability to exploit their trusted access to conduct adversary actions without compromising safety and security is difficult. A variety of approaches have been developed, however, and further development is ongoing.

Ensuring such creativity becomes an issue of organizational security culture, as some organizations tend to react against assessors and testers who regularly find weaknesses in the security system, rather than rewarding them. Organizations need to find ways to give people the mission and the incentives to find nuclear security weaknesses and suggest ways they might be fixed. But with the right approaches and incentives in place, effective vulnerability assessment and testing can be a key part of achieving and sustaining high levels of nuclear security.

## State

United States

## Gender

Male

**Primary authors:** BUNN, Matthew (Harvard University); ROTH, Nickolas (Belfer Center, Harvard University)

**Presenter:** ROTH, Nickolas (Belfer Center, Harvard University)

**Track Classification:** PP: Nuclear security vulnerability assessments