Best practices for securing critical/regulated infrastructures within the U.S.

Tom Mullen[1]
[1]*OPSWAT*

U.S. nuclear power facilities use digital and analog systems to monitor, operate, control, and protect their plants. "Critical digital assets" that interconnect plant systems performing safety, security, and emergency preparedness functions are isolated from the internet. This “air gap” separation provides protection from many cyber threats. Even so, all power reactor licensees must implement and maintain a cyber security plan under regulations by the U.S. Nuclear Regulatory Commission (NRC) addressing the transfer of digital content from one isolated network to another via portable media such as flash drives, USBs, and so forth.

Attendees will learn about processes adopted by reactor licensees to inspect portable media for cyber threats that satisfy U.S. NRC regulation and how such processes have been adopted, as a best practice, by (1) nuclear power generation facilities in EMEA and APAC, (2) non-nuclear power generation facilities owned by energy companies and utilities holding power reactor licenses in the U.S., and (3) other operators of facilities relying upon air-gapped networks.