

## Quantum-Resistant Security

### Bill Becker

Vice President of Product Management  
Thales Trusted Cyber Technologies

Quantum computing is advancing rapidly, and its impact is likely to be large. Their potential computational power could render today's encryption algorithms obsolete.

Quantum computers can launch attacks that break asymmetric cryptography, rendering the entire PKI-based encryption method obsolete. In fact, the National Institute of Standards and Technology (NIST) is researching way to deal with the effects of quantum power.

As quantum technology advances, agencies will be forced to protect their information and communications against cryptographic attacks through quantum resistant technology.

Attend this session to learn how to stay one-step ahead of the quantum risk by deploying future-proof encryption technology to protect your data. This session will discuss:

- Overview of the security risks posed by quantum computers
- National quantum initiatives
- Crypto agility