Business Software Alliance

From Legacy to Leadership

Why Modernizing Federal IT Is Essential for Meeting Quantum Threats

The Federal Government's outdated and bespoke information technology (IT) systems are increasingly at risk of, or are already unable to, withstand today's most sophisticated cyber threats. These threats are not only growing in scale and complexity, but they are also evolving faster than legacy systems can adapt. The mismatch between aging infrastructure and modern threats puts personal information and national security at risk.

It is imperative that the Federal Government modernize its IT.

Preparing for Quantum Computing

In addition to the current challenge created by outdated IT, a new threat is on the horizon: the approaching reality of a cryptographically relevant quantum computer, that is, a quantum computer that will be able to break today's most widely used encryption. While these computers do not yet exist, experts agree that their development is inevitable.

Even now, adversaries are employing a "harvest now, decrypt later" strategy: stealing encrypted data today with the intent to decrypt it once the quantum technology becomes available. This situation puts sensitive information, including personal and national security information, at risk today.

To counter the threat posed by a cryptographically relevant quantum computer, both the government and the private sector must upgrade to post-quantum cryptography (PQC): encryption designed to thwart quantum computers. Upgrading to PQC is a complex undertaking, and in many cases, agencies must first modernize their IT systems to support it.

As agencies plan their modernization strategies, they must ensure those efforts enable a timely upgrade to PQC.

Legacy IT Systems and PQC

Many legacy IT systems lack the processing power, memory, and architecture needed to implement post-quantum cryptography. Attempting to deploy PQC on these systems would be like trying to stream 4K video over a dial-up internet connection, the infrastructure simply can't support it.

As agencies plan their modernization strategies, they must ensure those efforts enable a timely upgrade to PQC. One path to that outcome is to leverage multiple cloud platforms that embed PQC, thereby streamlining agencies' modernization, while also allowing for different software needs.

The threat is not distant. Sensitive data stolen today may be decrypted tomorrow. Without forward-looking modernization, agencies risk investing in systems that are vulnerable from the moment they're deployed.

Moving From Legacy to Leadership

It's not enough for the Federal Government to modernize, it should lead. To ensure agencies are able to promote current capabilities while defending against future threats, the cost of upgrading to PQC should be reflected in their budget submissions, and further, BSA recommends they should:

1. Increase targeted funding to modernize legacy IT systems, including migrating to cloud platforms, enabling agencies to maintain cybersecurity and adopt emerging technologies such as post-quantum cryptography, artificial intelligence, and cloud-based tools.
2. Establish multi-year funding mechanisms to move from outdated infrastructure to modern, agile systems that can accommodate continuous software updates and evolving security requirements.
3. Expand the use of shared services to reduce duplication, accelerate modernization across agencies, and facilitate secure data sharing among federal, state, local, tribal, and territorial governments.

KEY TAKEAWAYS

1. Federal IT modernization is necessary and urgent.
2. Quantum computing poses economic and national security threats.
3. Strategic leadership and investment are essential.