QUANTUM COMPUTING FOR GOVERNMENT: EVIDENCE AND DECISIONS · PAPER 1

Quantum Computing for Government: What Is Demonstrated, What Is Projected, and What Remains Uncertain

Yuval Boger, QuEra Computing | November 2026 | Information current as of November 11, 2026 *Prepared with support from QuEra Computing.*

Executive summary

Quantum computing is advancing, and government already has good reasons to engage. The science is real, federal policy has set goals, and decisions about research, skills, and security are being made now. The difficulty is that announcements mix three different things: what has been demonstrated, what technical analysis projects for future machines, and what organizations say they plan to build. This paper offers a simple way to tell them apart. As of November 2026, researchers have demonstrated key building blocks of reliable quantum computing. No publicly documented quantum computer yet delivers routine results for a government mission that conventional computers cannot match, and no one can say reliably when that will change. The sensible course is to engage in stages: ask what kind of evidence stands behind each claim, build the capacity to evaluate claims, and fund learning with clear decision points. Cybersecurity upgrades should proceed independently, on their existing schedule.

What quantum computers are for

Most modern, classical computers do familiar jobs faster. Quantum computers are different. They are being built to solve a small number of problem types that conventional computers handle poorly. The National Academies concluded in 2019 that they are unlikely to replace conventional machines and will instead work alongside them as specialized accelerators [1]. Two kinds of problems motivate most of the investment. The first is simulating how molecules and materials behave, which matters for energy, medicine, and manufacturing. The second is a group of mathematical problems that includes breaking widely used cryptography that protects today's digital communication [1]. For other popular ideas, such as faster logistics planning or better artificial intelligence, the case is less settled [1].

The main obstacle is reliability. A quantum computer stores information in qubits, its basic working units, and qubits are far more easily disturbed than the bits in a conventional chip. Useful calculations need many more steps than today's qubits can complete without an error creeping in. The remedy is quantum error correction, which combines many physical qubits into one more reliable "logical" qubit, at a substantial cost in hardware [1]. Much of the field's current work is about making that remedy practical. In the meantime, today's machines serve mainly as research tools.

Three technologies that are often confused

Several technologies share the word "quantum" and mature at different rates. A good first question about any announcement is which one it concerns.

Quantum sensing measures time, motion, or magnetic fields with great precision. Some quantum sensors are already in everyday use: atomic clocks support GPS, and MRI machines rely on a related

effect [2]. A June 2026 executive order directs the Secretary of War (the title the order uses) to choose at least three newer sensor projects to field by September 30, 2028 [3].

Quantum networking links quantum devices to one another. The same order asks the Department of Energy for a five-year plan that includes using networks to connect quantum computers [3], which suggests this capability is still at the planning stage.

Post-quantum cryptography is often mistaken for a quantum technology. It uses new mathematical methods, running on ordinary computers, to protect information and verify authenticity, and it is designed to withstand attacks by future quantum computers. Federal agencies already have deadlines for adopting it [4], so this work does not wait on any quantum hardware.

How to read an announcement

Headlines rarely say what kind of evidence stands behind a claim. Table 1 sorts claims into four levels. Medicine offers a helpful comparison: a laboratory result, a clinical trial, and an approved treatment are all real progress, but they support different decisions. Quantum computing has no regulator to make those calls, so readers need to ask the questions themselves.

Table 1. Four levels of evidence (examples as of November 2026)

Level	What it tells you	What to ask	Example
Proposal	Something could work in theory on a future machine	What machine does it assume, and does that machine exist?	Estimates of the machine needed to break widely used cryptography [5]
Experiment	A capability was shown on real hardware	At what scale, and under what conditions?	Error correction that improves as the system grows [6]; calculations on error-protected qubits [7]
Benchmark	Performance was measured on a defined test	Compared with what, and has anyone independently checked it?	A 2026 sampling test, revised after independent researchers found a faster conventional way to analyze its outputs [8]
Routine mission advantage	A mission relies on results that conventional computers cannot match	Is it better than the conventional alternative at comparable cost?	None publicly documented; today's machines operate as research services [9]

Each level is real progress, and reaching one does not guarantee the next. Details and figures are in the technical note.

Real progress has been made at the experiment level. Google showed that an error corrected memory became more reliable as it was made larger, which is exactly what error correction is supposed to do [6]. A Harvard-led team that included researchers from MIT and QuEra ran calculations on dozens of error-protected logical qubits [7]. These are meaningful steps toward reliable machines. Neither was a useful application, and neither team claimed one.

Benchmark claims deserve particular care, because conventional computing keeps improving too. In July 2026, IBM and University of Chicago researchers reported a test calculation that they estimated was beyond the reach of conventional computers. Within weeks, independent researchers found a more efficient conventional method for analyzing the experiment's published outputs. Their work also supported its accuracy estimate, and the authors revised the experiment around a harder test [8]. The exchange shows why open data and independent scrutiny matter. For officials, the lesson is to ask whether a claim has been independently tested before relying on it.

The top level is still empty: no mission is known to depend on results that only a quantum computer can provide. Quantum computers are available today as research services. QuEra's Aquila, for example, has been offered through Amazon's cloud service since 2022 [9]. As of November 2026, we are not aware of a publicly documented case in which a quantum computer routinely delivered mission results that conventional methods could not match at comparable cost. The Defense Advanced Research Projects Agency (DARPA) runs a program, the Quantum Benchmarking Initiative, to test whether any approach can deliver more value than it costs by 2033 [10].

What will set the pace

No one can reliably predict when quantum computers will deliver routine value. The National Academies recommended tracking measurable progress instead of forecasting dates [1], and that advice still holds. Three things are worth watching.

- **Reliability at scale.** The useful measure is how long a calculation a machine can finish correctly. A count of qubits, on its own, says little about that.
- **Smarter methods.** Better algorithms keep shrinking the machine a problem requires. One estimate of the hardware needed to break a widely used form of cryptography fell about twentyfold between 2019 and 2025, although the smaller machine would need to run longer [5].
- **The conventional competition.** Conventional computers and methods keep improving, so every claim of a quantum advantage is measured against a moving target [8].

What is worth doing now

Uncertainty about timing is not a reason to wait. Several activities can deliver value before routine quantum advantage arrives. Research access to today's machines lets scientists and agencies learn what the technology can and cannot do. Training builds a workforce able to use and evaluate it. Independent testing gives government its own view of what works. Identifying mission problems now means agencies will know what to ask for when more capable machines arrive. None of these depends on a specific delivery date.

Actions for government leaders

1. **Ask what kind of evidence it is.** Before citing an announcement in a briefing or budget justification, check whether it is a proposal, an experiment, a benchmark, or routine mission use, and whether independent experts have reviewed it.
2. **Ask what it was compared with.** A claim of quantum advantage needs a comparison with the best available conventional method, and that comparison can change quickly [8].
3. **Keep cybersecurity on its own track.** Federal policy sets deadlines in 2030 and 2031 for the most sensitive federal systems to adopt post-quantum cryptography, and older methods are to be retired after 2035 [4]. These dates do not depend on any hardware forecast.
4. **Build or borrow evaluation capacity.** Agencies need staff or advisers who can read the underlying research and test claims. The DARPA program is one model: a government team that examines companies' hardware and plans [10].
5. **Fund learning in stages.** Modest investments in training, problem selection, and access to current systems let an agency learn without betting on a single date or technology. Tie each stage to the evidence in Table 1, and revisit assumptions at least once a year.

Technical note: the numbers behind this paper

- **Error correction.** Google's 101-qubit error-corrected memory cut its logical error rate by a factor of about 2.14 each time the code was enlarged, reaching 0.143% per cycle. Rare correlated errors, about one per hour, limited a related test [6].
- **Logical qubits.** The Harvard-led experiment ran circuits with up to 48 logical qubits. It used codes that detect errors without correcting them and improved results by discarding runs with detected errors [7].
- **Benchmark case.** A second team computed the probabilities of all 2,051 published outputs of the original 70-qubit circuit in 37.3 minutes on 256 graphics processors, which also supported the experiment's accuracy estimate. The revised preprint leads with a 64-qubit circuit and keeps fewer than 4 of every 10,000 runs after its error checks [8].
- **Cryptography estimate.** For factoring a 2048-bit RSA key: about 20 million qubits running for eight hours (2019 estimate) versus fewer than one million running for under a week (2025 estimate), with the same assumptions, including a 0.1% error rate per operation. This is a modeled estimate in a preprint [5].
- **Cybersecurity dates.** High value assets and high impact federal systems must use post-quantum cryptography for key establishment by December 31, 2030 and for digital signatures by December 31, 2031. NIST will deprecate quantum-vulnerable public-key algorithms after 2030 and disallow them after 2035 [4].
- **Targets and definitions.** QuEra's stated target is more than 256 logical qubits and about one million reliable logical operations on Amazon Braket in 2028 (a vendor target) [9]. DARPA defines utility-scale operation as computational value that exceeds cost [10].

References

[1] National Academies of Sciences, Engineering, and Medicine. *Quantum Computing: Progress and Prospects.* The National Academies Press (2019). Report (National Academies). https://doi.org/10.17226/25196

[2] National Science and Technology Council, Subcommittee on Quantum Information Science. "Bringing Quantum Sensors to Fruition." (March 2022). U.S. government publication. https://www.quantum.gov/wp-content/uploads/2022/03/BringingQuantumSensorstoFruition.pdf

[3] Executive Order 14413. "Ushering in the Next Frontier of Quantum Innovation." The White House (June 22, 2026). U.S. government publication. https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-nextfrontier-of-quantum-innovation/

[4] Moody, D., Perlner, R., Regenscheid, A., et al. "Transition to Post-Quantum Cryptography Standards." NIST IR 8547, National Institute of Standards and Technology (October 2026). U.S. government publication. https://csrc.nist.gov/pubs/ir/8547/final

[5] Gidney, C. "How to factor 2048 bit RSA integers with less than a million noisy qubits." arXiv:2505.15917 (2025). Preprint, not peer-reviewed. https://arxiv.org/abs/2505.15917

[6] Google Quantum AI and Collaborators. "Quantum error correction below the surface code threshold." *Nature* 638, 920-926 (2025). Peer-reviewed. https://doi.org/10.1038/s41586-024-08449-y

[7] Bluvstein, D., Evered, S. J., Geim, A. A., et al. "Logical quantum processor based on reconfigurable atom arrays." *Nature* 626, 58-65 (2024). Peer-reviewed. https://doi.org/10.1038/s41586-023-06927-3

[8] Martiel, S., Chung, J.-U., Seif, A., et al. "Sampling hard circuits with verifiably high fidelity." arXiv:2607.25941, version 3 (September 2026). Preprint, not peer-reviewed. https://arxiv.org/abs/2607.25941

[9] QuEra Computing. "QuEra Announces 2028 Fault-Tolerant Quantum Computer and Expanded Multi-Year Strategic Collaboration with AWS." Press release (June 15, 2026). Vendor publication (QuEra). https://www.quera.com/press-releases/quera-announces-2028-fault-tolerant-quantum-computer-andexpanded-multi-year-strategic-collaboration-with-aws

[10] Defense Advanced Research Projects Agency. "Four more teams enter Quantum Benchmarking Initiative's final stage." News release (October 7, 2026). U.S. government publication. https://www.darpa.mil/news/2026/fourmore-teams-enter-quantum-benchmarking-initiative-final-stage

About QuEra Computing

QuEra Computing builds neutral-atom quantum computers, drawing on research from Harvard and MIT. Its Aquila system has been available on Amazon Braket since 2022, and its Libra fault-tolerant system is planned for Amazon Braket in 2028. Learn more at www.quera.com.