

THIS WEEK IN QUANTUM SECURITY

September 25, 2026

By
Joel Van Dyk
Quantum Security Advisor
and Strategist

This week, quantum security looked less like a standards exercise/physics experiment and more like the beginnings of an engineering industry. Governments are moving into procurement and exercises, the US Department of Energy has launched a milestone-based competition for fault-tolerant quantum computers, IBM is building a dedicated quantum foundry, NVIDIA is pushing fault-tolerant architecture into the software stack, and the ITU has just completed a global drill focused on what breaks when post-quantum cryptography reaches real systems. At the same time, Quantum World Congress opens in Maryland with an agenda centered on commercialization, policy, workforce and scaling the infrastructure needed to support the quantum economy.

The common thread is that the machinery around quantum is being built now. A cryptographically relevant quantum computer has not arrived, but the systems, supply chains, procurement frameworks, software layers, exercises and industrial capacity required for quantum computing and post-quantum migration are moving quickly. For security teams, that makes the timeline question less useful than it once was. The harder question is whether organizations can move fast enough once the surrounding infrastructure starts changing around them.

The Week's Key Developments

The ITU Global Quantum Drill tested what happens when PQC reaches real systems

The ITU Global Quantum Drill took place in Dubai on 17–18 September, hosted by the UAE Cyber Security Council and preceded by regional ITU-T security meetings for Africa and the Arab region. The event was explicitly designed to let governments, national CERTs, technical teams and other participants assess readiness through simulated quantum-related cybersecurity scenarios rather than simply discuss standards.

One of the most useful scenarios focused on a distinction that is easy to miss in the migration debate: a strong cryptographic primitive does not automatically make the system around it secure. Participants were asked to analyse post-quantum mechanisms including FALCON and HAWK and identify weaknesses introduced through implementation, integration, protocol design, configuration, operational assumptions and information leakage. The ITU was explicit that the exercise was not about “breaking PQC” mathematically; it was about understanding the attack surface that appears once PQC is implemented inside real systems.

That is an important shift in emphasis.

Over the past two years, much of the industry's attention has naturally focused on algorithm selection and standardisation. As deployment begins, the more familiar security problems return: keys are

mishandled, protocols make assumptions that no longer hold, hardware leaks information, and migration layers create new complexity.

For security leaders, the lesson is practical. Quantum readiness is not complete when an approved algorithm has been selected. The organisation has to understand how the algorithm behaves in certificates, HSMs, endpoints, network protocols, identity systems and operational processes.

The drill also matters because it creates a common exercise model. Governments and critical-infrastructure organisations can now test not only whether they have a migration strategy, but whether their teams know how to respond when the threat model changes underneath a live system.

The US federal government is moving from PQC guidance into acquisition and implementation

The GSA Post-Quantum Cryptography Summit on 16 September brought together GSA, OMB, NIST, CISA and other federal agencies around migration strategy, identity, crypto-agility, implementation case studies and procurement. The event's learning objectives were unusually direct: understand federal migration priorities, explore the quantum-safe marketplace, examine PIV and identity impacts, develop crypto-agility strategies and identify acquisition pathways already available to agencies.

That is more significant than another federal awareness event.

Once procurement pathways appear, guidance starts to influence markets. Vendors have to design for the requirements agencies are actually allowed to buy, while federal programme managers can begin moving budget against migration work rather than waiting for another policy document.

Identity is also emerging as one of the harder areas. PIV, PKI and long-lived trust relationships tend to have more dependencies than a simple TLS update, and federal identity systems operate across organisational boundaries. That makes them a useful proxy for the broader enterprise problem.

The presence of both CISA and NIST also reinforces the implementation point from the ITU drill. PQC migration is increasingly about how standards are deployed and validated, not just which standards exist.

For suppliers, the useful question is becoming clearer: can they show that their products fit into a crypto-agile architecture, can they produce evidence of secure implementation, and can they support organisations through hybrid transition periods without creating new operational risk?

DOE puts up to \$215 million behind a race to fault-tolerant quantum computing

On 17 September, the US Department of Energy launched the Quantum Genesis Q Competition, with up to \$215 million in planned funding for private-sector companies capable of demonstrating scientifically relevant fault-tolerant quantum computers.

The programme is milestone-based. Phase I offers up to \$1.5 million per awardee for early milestones. Phase II creates a \$100 million incentive pool for companies that can demonstrate a first-generation system with at least 100 logical qubits, with additional \$50 million pools for systems reaching 150 and 200 logical qubits. DOE says the target systems should be capable of hundreds of millions of fault-tolerant operations.

That is a more meaningful signal than many headline qubit announcements.

Physical qubit counts can be misleading because useful fault-tolerant computation depends on error correction, logical-qubit quality, gate fidelity, efficient programs/algorithms and the ability to run long computations reliably. By tying funding to logical qubits and fault-tolerant operations, DOE is effectively defining the milestones it believes matter for scientifically useful quantum computing.

This should still not be translated into a new Q-Day date. A 100(or 1000)-logical-qubit scientific system is not automatically a cryptographically relevant machine, and the engineering distance between the two can still be substantial.

What the programme does show is that government funding is becoming more explicit about the path from experimental hardware toward fault-tolerant systems.

For quantum-security programmes, that makes the direction of travel easier to see. The uncertainty is increasingly about timing and architecture, not whether governments and major vendors intend to build systems capable of operating beyond today's noisy quantum regime.

IBM and Anderon turn quantum hardware into a manufacturing story

On 16 September, Anderon, an IBM company, finalised a \$1 billion CHIPS award with the US Department of Commerce to expand quantum-wafer R&D and manufacturing in Albany, New York. IBM is backing the venture with another \$1 billion of its own capital.

Anderon operates what IBM describes as a 300mm pure-play quantum wafer foundry intended to provide manufacturing capability to customers across the quantum ecosystem rather than only to IBM's internal programmes.

This matters because one of the less visible constraints on quantum computing is repeatable manufacturing.

A laboratory can produce a small number of specialised devices. An industry needs wafers, fabrication processes, packaging, yield management, test infrastructure and supply chains that can produce devices reliably and at scale.

The US government is therefore not simply funding quantum-algorithm research. It is investing in the semiconductor infrastructure required to support a domestic quantum hardware industry.

That industrial layer matters for security because it changes the nature of the signal.

Quantum computing is increasingly being treated in the same policy category as advanced semiconductors, AI infrastructure and other strategically important technologies. Governments are building the production capacity long before fault-tolerant systems are commercially mature.

The relevant point for cybersecurity teams is not that IBM's foundry creates an immediate cryptographic threat. It is that the organisations trying to build large-scale quantum systems are investing in the manufacturing bottlenecks now rather than waiting for the technology to be finished.

Fault-tolerant quantum computing is becoming a software problem as well as a hardware problem

NVIDIA published CUDA-Q Logical on 14 September, a retargetable compilation framework for fault-tolerant quantum computing.

The framework is designed to compile quantum workloads through logical circuits, error-correction codes and hardware assumptions while producing resource estimates directly from compiler artefacts. NVIDIA's researchers argue that this allows teams to compare architectures more consistently and identify cost drivers that can be hidden by simplified analytical models.

Australia's Iceberg Quantum and Diraq have already used the platform to evaluate fault-tolerant spin-qubit architectures. Iceberg Quantum says its Pinnacle architecture is designed around qLDPC codes that substantially reduce error-correction overhead, while the NVIDIA work lets teams test those claims against a common compilation environment.

This is worth following because the path to fault tolerance is not simply a race to fabricate more qubits.

A useful system has to map algorithms through logical qubits, error-correction codes, scheduling, routing and physical hardware. Tooling that lets researchers model that entire n-dimensional stack is part of the engineering infrastructure needed to make fault-tolerant systems buildable.

The software layer is also becoming strategically important. France's CEA and Alice & Bob announced a collaboration around Qaptiva, an open-source quantum-supercomputing software environment intended to connect classical supercomputers and quantum processors. CEA has been explicit that Europe should avoid recreating the dependence on a single software platform that has emerged around AI compute.

That introduces another dimension to the quantum-industrial discussion: who controls the software layer through which future quantum hardware is programmed, benchmarked and integrated with classical computing?

Global Signals

North America

North America is where the week's industrial and policy story is most visible.

The DOE competition, GSA summit and Anderton foundry all point in the same direction: federal quantum policy is moving from research support and migration guidance into procurement, manufacturing and explicit engineering milestones.

The next major gathering is Quantum World Congress, 23–25 September, in College Park, Maryland. The organisers describe it as the point where research, policy, investment, workforce and industry meet to define the next stage of the quantum economy. Major hardware companies, technology firms, government organisations and investors are expected to participate.

That framing is worth paying attention to.

The conversation around quantum is increasingly less about demonstrating that the science works and more about how the industry scales: manufacturing, error correction, hybrid integration, workforce, capital and national strategy.

The security question should sit inside that same discussion. A quantum economy built without a corresponding plan for cryptographic transition would simply move one side of the technology faster than the other.

United Kingdom and Europe

Europe is increasingly treating quantum software, identity and trust infrastructure as strategic layers.

CEA and Alice & Bob's Qaptiva work reflects a concern that Europe should not become dependent on one dominant quantum-computing software stack. The collaboration will connect classical HPC and quantum systems and is being positioned as part of a broader sovereign-computing strategy.

ENISA's Trust Services and eID Forum in Tallinn also placed the potential effects of post-quantum cryptography directly into the digital-identity conversation. That matters because European identity wallets, trust services and certificate infrastructure will have to migrate without breaking interoperability across member states.

This is a different challenge from simply replacing a server certificate. Identity systems involve long-lived credentials, regulatory requirements, cross-border trust and large numbers of relying parties.

Europe's migration challenge is therefore increasingly about coordination between standards, regulation and infrastructure rather than simply adopting NIST algorithms.

Asia

The strongest Asian signals continue to come from financial infrastructure, manufacturing and standards participation.

India's recent Reserve Bank push for a Quantum Secure and Adaptive Financial Ecosystem remains important because it places one of the world's largest digital-payment environments into an explicit quantum-readiness programme.

Across the wider region, semiconductor and hardware ecosystems in Japan, South Korea and Taiwan continue to make quantum and post-quantum security part of strategic technology planning.

The more interesting shift is that Asian activity increasingly spans both sides of the problem: building quantum computing capability while also embedding quantum-safe security into PKI, hardware roots of trust and financial infrastructure.

That dual-track model is probably where most major economies will eventually end up.

Australia

Australia produced two useful commercialisation signals this week.

Quantum Australia launched a Quantum Commercial Pilot Challenge on 17 September, inviting organisations to submit real commercial or operational problems that could benefit from quantum computing. Selected projects receive funded quantum-compute access and are expected to define a classical benchmark, measurable outcome and a clear pathway to a larger pilot or commercial decision. Applications close on 15 October.

That is a useful model because it forces the quantum proposition to compete against an existing classical solution rather than simply demonstrating that a quantum workload can run.

Australia is also home to the Iceberg Quantum/Diraq fault-tolerance work using NVIDIA CUDA-Q Logical, while Diraq is preparing to place a silicon-spin quantum system inside an Equinix commercial data centre in Sydney.

Together, those developments show Australia trying to close the gap between research and commercial infrastructure while its government maintains one of the clearer post-quantum migration timelines internationally.

Africa

Africa deserves more than the usual “no announcement this week” line.

At the ITU-T Regional Group for Africa meeting on 16 September, Guinea submitted a formal contribution titled “Preparation of African countries for post-quantum cybersecurity of critical digital infrastructures.” Guinea also submitted a broader update on its domestic cybersecurity position.

That is significant because it shows PQC preparedness becoming an explicit regional standards and policy topic rather than something imported later from Europe or North America.

Africa does not need a domestic fault-tolerant quantum computer for quantum migration to matter. Telecom networks, banking systems, government identity infrastructure and cloud services already depend on vulnerable public-key cryptography.

Regional coordination through the ITU may therefore be one of the more important mechanisms for avoiding a fragmented migration.

Middle East

Dubai has become an unusually important convening point for practical quantum-security activity.

The ITU drill brought governments, national cyber authorities, technical teams and standards organisations together around operational readiness rather than general awareness. That is a meaningful development for a region already investing heavily in sovereign quantum capability.

The next regional event is the Quantum Innovation Summit in Dubai from 28–30 September.

The useful question there will be whether the discussion moves beyond hardware investment and national ambition into concrete procurement, migration programmes and operational quantum-security requirements.

Latin America

Brazil produced the strongest Latin American hardware signal this week.

IQM announced that it will deliver an IQM Spark quantum computer to the Eldorado Research Institute in Campinas in the first quarter of 2027. The agreement also includes cloud access to IQM’s larger European systems and is intended to make quantum hardware available to Brazilian universities, researchers, startups and industrial partners.

This is IQM’s first quantum-computer sale in South America and is a useful regional milestone because it gives local researchers and companies direct access to on-premises hardware rather than relying entirely on overseas cloud systems.

It does not create a cryptographic threat in Brazil.

It does create local capability, training and infrastructure, which are the ingredients from which a domestic quantum ecosystem develops.

Research Worth Reading

“CUDA-Q Logical: Retargetable Compilation for Fault-Tolerant Quantum Computing.” NVIDIA’s paper is worth reading because it treats fault tolerance as a full-stack engineering problem. The framework connects application workloads, logical circuits, error correction, scheduling and physical architectures so that resource estimates can be compared on a common basis. The limitation is that these remain models of future fault-tolerant systems rather than demonstrations on hardware at the required scale.

Cloudflare — “1.1.1.1 now supports post-quantum DNSSEC, all 2,420 bytes of it.” Cloudflare has enabled validation of DNSSEC signatures made with ML-DSA-44 on its public resolver. The interesting part is not simply that ML-DSA works. The 2,420-byte signature size exposes exactly the sort of transport and protocol constraints that appear when PQC moves beyond TLS into internet infrastructure. Cloudflare describes this as an early step toward its broader goal of full post-quantum security by 2029.

Anthropic — “Detecting and countering misuse of AI: September 2026.” Anthropic reports that AI is increasingly being used not only to assist cyber operators but to orchestrate vulnerability research and exploitation workflows. The company says it has seen automated “exploit foundries” and cases where comparatively unsophisticated operators used AI to sustain complex campaigns. These are Anthropic’s observations from activity on its own systems, not an independent measurement of the entire threat landscape, but they are relevant to the security of new PQC implementations.

Anthropic — “An alignment assessment of recent cybersecurity incidents.” The assessment covers four incidents in which Claude models gained unauthorised access to real third-party systems during evaluation environments. Anthropic says it expanded its review to roughly 481 million transcripts after identifying the incidents. This is not quantum research, but it is useful context for why implementation quality and system isolation matter as increasingly autonomous AI systems become capable cyber actors.

Meetings and Events to Watch

23–25 September — Quantum World Congress, College Park, Maryland. This is the main event to watch this week. The programme brings together quantum hardware companies, technology firms, government, investors and universities around commercialization, workforce, policy and scaling the quantum economy. The useful signals will be manufacturing commitments, named customers, error-correction progress and evidence of real commercial deployment rather than stock-market reaction.

28–30 September — Quantum Innovation Summit, Dubai, UAE. After the ITU Global Quantum Drill, this will be the next major Middle East gathering. Watch for national quantum-readiness programmes, security procurement and concrete infrastructure commitments rather than broad investment announcements.

15 October — Quantum Australia Commercial Pilot Challenge application deadline. The programme is seeking problems with defined owners, data, classical benchmarks and measurable business outcomes. The structure itself is worth watching because it forces quantum pilots to prove value against an existing baseline.

What to Watch Next

Quantum World Congress is the obvious focus over the next few days.

The event's public framing is telling. It is not primarily asking whether quantum computing is real. It is asking how to build the quantum economy: how the technology is manufactured, financed, commercialised, integrated with classical infrastructure and supported by a sufficiently skilled workforce.

That does not mean the commercial problem has been solved. Quantum-company revenues remain small relative to valuations and capital requirements, and fault-tolerant systems remain engineering targets rather than finished products.

The useful question is whether the conversation now produces evidence of repeatable demand.

Named customers matter. Renewals matter. Manufacturing yield matters. Error-correction milestones matter. Software that works across multiple hardware architectures matters. Government procurement that moves beyond pilot programmes matters.

On the security side, the ITU drill and GSA summit have made something else clearer.

PQC is entering the phase where secure implementation becomes as important as algorithm selection.

Cloudflare's DNSSEC work gives a simple example: a standardised signature can still change packet sizes, transport behaviour and protocol assumptions. The ITU drill makes the same point from an attack perspective: the mathematics may be sound while the system remains vulnerable.

That is where AI increasingly enters the discussion as well.

Anthropic is now reporting AI systems being used to automate exploit research and orchestrate attacks, while security vendors are building multi-model defensive systems to try to operate at the same speed.

None of that means AI has broken PQC.

It means that the systems implementing PQC will be attacked by increasingly capable automation.

Taken together, the week points to something larger than another round of quantum announcements.

The world is beginning to build the industrial, software, procurement and security machinery around quantum computing.

The technology is still developing.

The infrastructure around it is already becoming real.

— Joel Van Dyk

Source Links

1. <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2026/0916/Pages/default.aspx>
2. <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2026/0916/Pages/programme.aspx>
3. <https://www.gsa.gov/events/2026-postquantum-cryptography-summit-in-person-91626>

4. <https://www.energy.gov/science/articles/doe-launches-competition-accelerate-development-worlds-first-fault-tolerant>
5. <https://newsroom.ibm.com/2026-09-16-anderson%2C-an-ibm-company%2C-finalizes-agreement-with-the-u-s-department-of-commerce-for-a-1-billion-chips-award-to-accelerate-r-d-for-u-s-based-pure-play-quantum-foundry>
6. <https://www.nist.gov/news-events/news/2026/09/departments-commerce-announces-finalization-chips-rd-award-anderson>
7. https://research.nvidia.com/publication/2026-09_cuda-q-logical-retargetable-compilation-fault-tolerant-quantum-computing
8. <https://www.reuters.com/technology/frances-cea-alice-bob-partner-quantum-supercomputing-software-2026-09-17/>
9. <https://www.enisa.europa.eu/events/trust-services-and-eid-forum-ca-day-2026>
10. <https://quantumworldcongress.squarespace.com/2026>
11. <https://www.investors.com/news/technology/quantum-computing-stocks-world-quantum-conference-2026/>
12. <https://www.quantum-australia.com/news/quantum-commercial-pilot-challenge>
13. <https://www.iceberg-quantum.com/>
14. <https://newsroom.equinox.com/2026-09-01-Dirac-and-Equinox-to-Deploy-Australias-First-Quantum-Computer-Inside-a-Data-Centre>
15. <https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17RG.AFR-260916-C&source=Guinea>
16. <https://iqm.gcs-web.com/news-releases/news-release-details/iqm-deliver-its-first-quantum-computer-south-america-brazils>
17. <https://blog.cloudflare.com/post-quantum-dnssec-1111/>
18. <https://www.anthropic.com/threat-intelligence-report-september-2026>
19. <https://www.anthropic.com/research/alignment-assessment-cybersecurity-incidents>