G7 Cyber Expert Group Recommends Action to Combat Financial Sector Risks from Quantum Computing WASHINGTON – The G7 Cyber Expert Group (CEG) – chaired by the U.S. Department

September 25, 2024

WASHINGTON – The G7 Cyber Expert Group (CEG) - chaired by the U.S. Department of the Treasury and the Bank of England - released a public statement today highlighting the potential cybersecurity risks associated with developments in quantum computing and recommending steps for financial authorities and institutions to take to address those risks.

Quantum computers are being built that will be able to solve computational problems currently deemed impossible for conventional computers to solve within a reasonable amount of time. While potentially providing significant benefits to the financial system, these powerful computers will also carry with them unique cybersecurity risks. One of the most significant is that cyber threat actors could use quantum computers to defeat certain cryptographic techniques that secure communications and IT systems, potentially exposing financial entity data, including customer information.

"The G7 CEG looks to help support the responsible use of emerging technologies like Cloud, AI, and Quantum in the financial sector while balancing the risks to the global economy," said Treasury Deputy Assistant Secretary for Cybersecurity and Critical Infrastructure Protection Todd Conklin, Co-Chair to the G7 CEG. "Cyber experts across the financial sector have developed internal plans related to quantum innovation and resilience, and it is critical that they obtain the support needed for their successful implementation. The G7 CEG believes that planning for the quantum transition is important to economic security and prosperity, and strongly encourages financial institutions to provide funding and other resources needed to support it."

While the exact timeline for developing quantum computers with these capabilities is uncertain, there is a real possibility that such capabilities could emerge within a decade. These quantum computers would not only put future data at risk, but also any previously transmitted data that cyber adversaries have been able to intercept and store with the intent

of decrypting later with quantum computers. Due to the potentially long lead time needed to put in place quantum-resilient technologies, the time to start planning is now.

An initial set of quantum-resilient encryption standards was released by the National Institute of Standards and Technology (NIST) last month. Additional standards from NIST and other standard-setting bodies are expected in the future. It is important for financial entities to maintain the agility required to incorporate new encryption standards in a timely and appropriate manner as they become available.

With the availability of NIST's standards, some financial entities may be in a position now to start making the needed changes to implement quantum resilient technologies within their systems. Others may be dependent on vendors and other third parties to develop implementations of the new standards that can be incorporated once they become available. No matter where entities are in their adoption timelines, the G7 CEG strongly encourages financial authorities and institutions to begin taking the following steps to build resilience against quantum computing risks:

1. Develop a better understanding of the issue, the risks involved, and strategies for mitigating those risks.
2. Assess quantum computing risks in their areas of responsibility.
3. Develop a plan for mitigating quantum computing risks.

The CEG statement provides additional details on quantum computing risks and the specific actions that financial entities can start taking to build quantum resilience within the financial system.

The G7 CEG's membership includes representatives of financial authorities across all G7 countries as well as the European Union. It was founded in 2015 to serve as a multi-year working group that coordinates cybersecurity policy and strategy across the member jurisdictions. In addition to policy coordination, the G7 CEG also acts as a vehicle for information sharing, cooperation, and incident response.

###