G7 2026 Cross Border Coordination Exercise (CBCE)

PRESS RELEASE

The G7 Cyber Expert Group (CEG) successfully concluded its 2026 Cross-border-coordination exercise (CBCE) on May 18, 2026. This exercise demonstrates the Group's ongoing commitment to strengthening cyber resilience across the G7 financial sector. A long-term exercise strategy has now been adopted to increase the frequency and consistency of these simulations, thereby enhancing preparedness across all jurisdictions.

Building on the success of the 2024 CBCE exercise, which aimed to strengthen the G7 financial authorities' capacity to coordinate and communicate effectively in response to a major cross-border cyber incident affecting the financial sector, this year's sessions tested key improvements identified through previous simulations and workshops focused on incident response, recovery, and crisis communication, further advancing collective preparedness. To enhance coordination among G7 financial authorities, the exercise simulated a large-scale cyber-attack across all G7 jurisdictions. The scenario brought together ministries of finance, central banks, bank supervisors, and market authorities, fostering a unified response.

Through these exercises, the G7 Cyber Expert Group seeks to reinforce the financial sector's capacity to withstand cyber threats and reduce potential disruptions across G7 jurisdictions. Bank of England Deputy Governor for Monetary Policy, Clare Lombardelli, said, "Our financial system, and the technologies it uses, are international. Disruption from cyber-attacks on our systems can cross borders, making a coordinated international response essential. We must have the right tools and resources to respond together when a crisis occurs, and I welcome the G7 CEG's work to build our shared capability."

This initiative enables financial authorities to further align and integrate the various operational and strategic components required for an effective response to cyber incidents.

In an increasingly interconnected world, cross-border coordination, incident response preparedness, and timely information sharing remain key G7 priorities. The G7 Cyber

Expert Group continues to work and collaborate to address potential cyber threats to safeguard the stability and integrity of the global financial system.

“Cyber threats do not respect borders, and neither can our response,” commented PDO Deputy Secretary Francis Brooke. “The G7 Cross-Border Coordination Exercise strengthens our collective ability to respond to cyber incidents that could affect the global financial system. As the United States prepares to assume the G7 Presidency, the U.S. Department of the Treasury looks forward to deepening practical cooperation through the G7 Cyber Expert Group and advancing a more secure and resilient global financial system.”

About the G7 Cyber Expert Group

The G7 Cyber Expert Group is responsible for coordinating cybersecurity policy and strategy across the G7 jurisdictions. Its mission is to enhance the cyber resilience of the financial sector by fostering preparedness, establishing a shared understanding of the threat landscape, and promoting unified approaches to risk mitigation.

Recent G7 Cyber Expert Group publications include:

- G7 Cyber Expert Group Statement on AI and Cybersecurity (2025)
- G7 CEG Reconnection Framework Best Practice (2025)
- G7 Cyber Expert Group statement on transition to post-quantum cryptography (2026)

For more information about the G7 Cyber Expert Group and its publications, please visit the webpage.