G-7 Finance Ministers and Central Bank Governors
Next Steps for Strengthening International Financial Sector Cyber Resilience
Backgrounder
October 2018

Improving the cyber resilience of the financial sector remains a priority for G-7 countries. The G-7 Cyber Expert Group (CEG) continues to support G-7 Finance Ministers and Central Bank Governors efforts to facilitate coordination across members and develop effective practices for cyber resilience in the finance sector.

Last year, G-7 Finance Ministers and Central Bank Governors published the *Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector*, which provided entities with a set of outcomes demonstrating good cybersecurity practices, as well as a set of non-prescriptive, not legally binding, high-level elements to use when assessing their level of cybersecurity. These fundamental elements can be useful to both public and private entities when considering effective practices for threat-led penetration testing and managing third party cyber risk in the financial sector.

Today two fundamental elements are published – *Fundamental Elements for Threat-led Penetration Testing* and *the Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector.*

The *Fundamental Elements for Threat-led Penetration Testing* provide organizations with a guide to assess their resilience against cyber-incidents by using simulated events. The *Fundamental Elements for Threat-led Penetration Testing* set out six core elements for entities and authorities to use when designing, implementing, and managing such tests. These cover: (1) Scoping and Risk Management; (2) Resourcing; (3) Threat Intelligence; (4) Penetration Testing; (5) Closure; and (6) Thematic Data.

The *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector* provide best practices to manage cyber risks posed by third parties to both private and public entities in the financial sector; they propose high-level elements for organizations to use as part of their third party cyber risk management practices. They set out six core elements for entities and authorities to manage third party cyber risk, covering: (1) Governance; (2) Risk Management Process for Third Party Cyber Risk; (3) Incident Response; (4) Contingency Planning; (5) Monitoring for potential Systemic Cyber Risk; and (6) Cross-sector Coordination.

Looking ahead, the Cyber Expert Group will continue to support Finance Ministers and Central Bank Governors by undertaking activities to promote cyber resilience in the financial sector. This includes further work to enhance situational awareness and coordination for responding to cyber incidents through a cross-border cyber crisis simulation exercise involving G-7 financial authorities and enhancing engagement among G7 financial authorities and private stakeholders.