28 June 2017

Progress Update on Cybersecurity Stock-Take

Report to 7-8 July 2017 G20 Leaders' Summit, Hamburg, Germany

The Communiqué issued at the March meeting of the G20 Finance Ministers and Central Bank Governors in Baden-Baden noted that the malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability. The Ministers and Governors further noted that they will promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20. With the aim of enhancing cross-border cooperation, the FSB was asked, as a first step, to perform a stock-take of existing relevant released regulations and supervisory practices in G20 jurisdictions, as well as of existing international guidance, including to identify effective practices. The FSB also was asked to inform about the progress of this work by the Leaders' Summit in July 2017 and deliver a stock-take report by October 2017. This note provides the requested progress update, including a description of steps taken and a description of next steps.

1. Steps Taken

In early April, the FSB initiated the requested stock-stake by distributing two surveys to its members for completion by 22 May. One survey was directed to FSB member jurisdictions, and the second survey was directed to international bodies that are FSB members.

The jurisdiction survey requested information about existing publicly released regulations, guidance and supervisory practices that address cybersecurity for the financial sector, including financial market infrastructures, trading venues, banks, insurance companies, broker-dealers, asset managers and pension funds. The survey addressed both schemes that (i) are targeted to cybersecurity risk; and (ii) address operational risk generally. The survey requested information about the matters addressed by the regulatory and supervisory schemes, as well as whether any existing national or international guidance or standards are incorporated, e.g. G7 Fundamental Elements of Cybersecurity for the Financial Sector or CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures. The survey also asked about (i) plans to issue new regulations, guidance or supervisory practices that address cybersecurity for the financial sector within the next year; and (ii) practices that jurisdictions deem effective in addressing cybersecurity through regulations, guidance and supervisory practices.

The international body survey asked about guidance that has been issued that addresses cybersecurity, as well as other documents relating to cybersecurity, including studies, surveys and reports. Like the jurisdiction survey, the international body survey addressed the financial sector, including financial market infrastructures, trading venues, banks, insurance companies, broker-dealers, asset managers and pension funds. Also similar to the jurisdiction survey, the international body survey requested

information about the matters addressed by guidance. The survey also asked about ongoing or planned work regarding cybersecurity.

All 25 FSB member jurisdictions have responded to the survey.[1] The 9 international body members that received the survey also have responded.[2] In addition, the G-7 Cyber Expert Group has submitted a response to the survey.

All jurisdictions report that they have publicly released regulations or guidance that address cybersecurity for at least a part of the financial sector. Many of these regulatory schemes are targeted to cybersecurity or information technology risk, while some address operational risk generally. A substantial majority of the responding jurisdictions report that they have publicly released supervisory practices that address cybersecurity for at least a part of the financial sector. Many jurisdictions report that their regulations, guidance and supervisory practices draw upon existing national or international guidance or standards of public authorities or private bodies, such as the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures, the U.S. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, or the International Organization for Standardization 27000 series (which provides information security control standards).

2. Next Steps

Over the coming months, the FSB will compile and analyse the responses into a report to be delivered to the G20 by October 2017 that provides cross-jurisdictional, cross-sectoral information about existing publicly available cybersecurity regulations, guidance and supervisory practices. The FSB also plans to hold a workshop in September, which will bring together public and private participants to discuss cybersecurity in the financial sector. Information gathered at the workshop also will be included in the report to be delivered to the G20 in October.

---

[1] This includes Argentina, Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, United Kingdom, United States and the European Union.

[2] The member international bodies that have responded are the Basel Committee on Banking Supervision, Committee on the Global Financial System, Committee on Payments and Market Infrastructures, International Association of Insurance Supervisors, International Accounting Standards Board, International Monetary Fund, International Organization of Securities Commissions, Organisation for Economic Co-Operation and Development and the World Bank.