G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR

Increasing in sophistication, frequency, and persistence, cyber risks are growing more dangerous and diverse, threatening to disrupt our interconnected global financial systems and the institutions that operate and support those systems. To address these risks, the below non-binding, high-level fundamental elements are designed for financial sector private and public entities to tailor to their specific operational and threat landscape, role in the sector, and legal and regulatory requirements.

The elements serve as the building blocks upon which an entity can design and implement its cybersecurity strategy and operating framework, informed by its approach to risk management and culture. The elements also provide steps in a dynamic process through which the entity can systematically re-evaluate its cybersecurity strategy and framework as the operational and threat environment evolves. Public authorities within and across jurisdictions can use the elements as well to guide their public policy, regulatory, and supervisory efforts. Working together, informed by these elements, private and public entities and public authorities can help bolster the overall cybersecurity and resiliency of the international financial system.

Element 1: Cybersecurity Strategy and Framework.
Establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines.

The purpose of a cybersecurity strategy and framework is to specify how to identify, manage, and reduce cyber risks effectively in an integrated and comprehensive manner. Entities in the financial sector should establish cybersecurity strategies and frameworks tailored to their nature, size, complexity, risk profile, and culture. Informed by the cyber threat and vulnerability landscape, a jurisdiction can also establish sector-wide cybersecurity strategies and frameworks that outline how cooperation occurs between entities and public authorities in the financial sector, with sectors upon which the financial sector depends, and with other relevant jurisdictions.

Element 2: Governance.
Define and facilitate performance of roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework to ensure accountability; and provide adequate resources, appropriate authority, and access to the governing authority (e.g., board of directors or senior officials at public authorities).

Effective governance structures reinforce accountability by articulating clear responsibilities and lines of reporting and escalation. Effective governance also mediates competing objectives and fosters communication among operating units, information technology, risk, and control-related activities. Consistent with their missions and strategies, boards of directors (or similar oversight bodies for public entities or authorities) should establish the cyber risk tolerance for their entities and oversee the design, implementation, and effectiveness of related cybersecurity programs.

Element 3: Risk and Control Assessment.
Identify functions, activities, products, and services—including interconnections, dependencies, and third parties—prioritize their relative importance, and assess their respective cyber risks. Identify and implement controls—including systems, policies, procedures, and training—to protect against and manage those risks within the tolerance set by the governing authority.

Ideally as part of an enterprise risk management program, entities should evaluate the inherent cyber risk (or the risk absent any compensating controls) presented by the people, processes, technology, and underlying data that support each identified function, activity, product, and service. Entities should then identify and assess the existence and effectiveness of controls to protect against the identified risk to arrive at the residual cyber risk. Protection mechanisms can include avoiding or eliminating risk by not engaging in an identified activity. They can also include mitigating the risk through controls or sharing or transferring the risk. In addition to evaluating an entity's own cyber risks from its functions, activities, products, and services, risk and control assessments should consider as appropriate any cyber risks the entity presents to others and the financial sector as a whole. Public authorities should map critical economic functions in their financial systems as part of their risk and control assessments to identify single points of failure and concentration risk. The sector's critical economic functions range from deposit taking, lending, and payments to trading, clearing, settlement, and custody.

Element 4: Monitoring.
Establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.

Effective monitoring helps entities adhere to established risk tolerances and timely enhance or remediate weaknesses in existing controls. Testing and auditing protocols provide essential assurance mechanisms for entities and public authorities alike. Depending on the nature of an entity and its cyber risk profile and control environment, the testing and auditing functions should be appropriately independent from the personnel responsible for implementing and managing the cybersecurity program. Through examinations, on-site and other supervisory mechanisms, comparative analysis of entities' testing results, and joint public-private exercises, public authorities can better understand sector-wide cyber threats and vulnerabilities, as well as individual entities' relative risk profiles and capabilities.

Element 5: Response.
Timely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders, third-party service providers, and customers as appropriate); and (d) coordinate joint response activities as needed.

As part of their risk and control assessments, entities should implement incident response policies and other controls to facilitate effective incident response. Among other things, these controls should clearly address decision-making responsibilities, define escalation procedures, and establish processes for communicating with internal and external stakeholders. Exercising protocols within and among entities and public authorities contributes to more effective responses. Exercising also enables entities and public authorities to identify how potential

decisions could affect each other's ability to maintain critical and other functions, services, and activities.

Element 6: Recovery.
Resume operations responsibly, while allowing for continued remediation, including by (a) eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d) remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally.

Once operational stability and integrity are assured, prompt and effective recovery of operations should be based on prioritization of critical economic and other functions and in accordance with objectives set by the relevant public authorities. Maintaining trust and confidence in the financial sector significantly improves when entities and public authorities have the ability to mutually assist each other in the resumption and recovery of critical functions, processes, and activities. Therefore, before an incident occurs, establishing and testing contingency plans for essential activities and key processes, such as funding, can contribute to a faster and more effective recovery.

Element 7: Information Sharing.
Engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents, and responses to enhance defenses, limit damage, increase situational awareness, and broaden learning.

Sharing technical information, such as threat indicators or details on how vulnerabilities were exploited, allows entities to remain up-to-date in their defenses and learn about emerging methods used by attackers. Sharing broader insights among entities, between entities and public authorities, and among public authorities deepens collective understanding of how attackers may exploit sector-wide vulnerabilities that could potentially disrupt critical economic functions and endanger financial stability. Given its importance, entities and public authorities should identify and address impediments to information sharing.

Element 8: Continuous Learning.
Review the cybersecurity strategy and framework regularly and when events warrant—including its governance, risk and control assessment, monitoring, response, recovery, and information sharing components—to address changes in cyber risks, allocate resources, identify and remediate gaps, and incorporate lessons learned.

Cyber threats and vulnerabilities evolve rapidly, as do best practices and technical standards to address them. The composition of the financial sector also changes over time, as new types of entities, products, and services emerge, and third-party service providers are increasingly relied upon. Entity-specific, as well as sector-wide, cybersecurity strategies and frameworks need periodic review and update to adapt to changes in the threat and control environment, enhance user awareness, and to effectively deploy resources. Other sectors, such as energy and telecommunications, present external dependencies; therefore, entities and public authorities should consider developments in these sectors as part of any review process.