Addressing Security and Privacy Challenges to Facilitate Regional Cross-Border Data Flows

Outcomes of the
Expert Roundtable on an APEC Data Ecosystem for Financial Services

March 2, 2019
Atlanta, Georgia
Regional Framework for Industry-Government Collaboration in Data Security

RECOMMENDATIONS:

• Establish a regional platform for public-private sector and relevant international organizations to:
  • Identify gaps in adoption of relevant international data security standards
  • Bridging the gaps through capacity building/technical assistance

• Develop innovative regional initiatives using new technologies for secure cross-border data flows
  • Example 1: Interbank Information Network (Led by JP Morgan, blockchain, banking)
    • [https://www.jpmorgan.com/global/treasury-services/IIN](https://www.jpmorgan.com/global/treasury-services/IIN)
  • Example 2: Proyecto Cadena (Led by IADB, blockchain, customs)

SOME KEY INTERNATIONAL DATA SECURITY STANDARDS

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002 on confidentiality, integrity and availability of data
- European Telecommunications Standards Institute (ETSI) Cyber Security Technical Committee (TC CYBER) standards,
- ISO/IEC 21827 governing organizations’ security engineering processes,
- Information Security Forum (ISF) Standard of Good Practices (SoGP) on management of information security risks in business organizations and their supply chains,
- US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF),
- ISO 15408 governing the integration and testing of software and hardware products,
- Internet Engineering Task Force (IETF) Site Security Handbook RFC 2196 providing a guide to setting computer security policies and procedures for sites that have systems on the Internet,
- IEC 62443 standards listing cybersecurity protection methods and techniques,
- Information Assurance for Small and Medium Enterprises (IASME) Governance standard for cybersecurity and protection of customer information in MSMEs participating in supply chains.
- ISO/IEC, American National Standards Institute (ANSI)/Society of Cable and Telecommunications Engineers, and the Institute of Electrical and Electronics Engineers (IEEE) on encryption and cryptography standards addressing algorithms, applications and related security considerations
APEC Privacy Regime

**RECOMMENDATIONS**

- Promote wider participation in CBPR (short-/medium-term target)
- Pathfinder initiative for inter-operable privacy regimes (long-term target)
  - Gap analyses of participating economies’ privacy regimes with APEC Privacy Framework
  - Identify provisions where:
    - Harmonization is needed
    - Derogations (exemptions) can be applied
  - Undertake needed legislative actions
- Negotiations for **inter-operability** with EU
- Public-private task force to **assist MSMEs** in complying with privacy rules
  - Best practices for MSMEs’ use of RegTech and LegalTech
  - Core data standards for MSMEs and limited safe harbor provisions for compliants
  - Identifying and vetting privacy enhancing technologies (PETs) for MSMEs to use in data pooling and sharing