5th Annual Technology and Justice for All CLE

COMPUTER AND TECHNOLOGY SECTION

Presented by the Computer and Technology Section of the State Bar of Texas
February 11, 2022

Emerging Global Cybersecurity Laws & Considerations for Int'l Businesses

COMPUTER AND TECHNOLOGY SECTION

Lavonne Burke Hopkins
Sr. Managing Legal Director, Security & Resiliency & IT
Houston, TX
Dell Technologies, Inc.

U.S. Executive Order on Improving the Nation's Cybersecurity (E.O. 14028)

White House issues Executive Order setting software security requirements for agencies and contractors

MAY 12, 2021 ORDER

In the wake of multiple significant cyberattacks and the breakdown of major IT systems, this order aims to create a means to prevent cyber disasters and/or limit their impact on Federal Information Systems and critical infrastructure

KEY PROVISIONS FOR GOVERNMENT

- Implementation of specific technical controls and architectures for Federal agencies required - multi-factor authentication, accelerate cloud adoption, zero trust architecture and data encryption
- Seeks to introduce "playbook" for government agencies' response to cyber incidents
- Sets up private-public sector Cyber Safety Review Board modeled on the National Transportation Safety Board to review large cyber incidents

KEY PROVISIONS FOR CONTRACTORS

- Requires IT and "**critical software**" providers contracting with government to meet higher security requirements
- Strict timelines for disclosing breaches
- Pilot of new star rating system for software sold to government

ATTACKS REFERENCED BY EO

SolarWinds

- Russian hackers targeted an update to a popular software to access thousands of companies and several US agencies

Microsoft Exchange

- Chinese state-backed hackers were conducting attacks by exploiting vulnerabilities in Microsoft software

Colonial Pipeline

- Ransomware attack on a key East Coast pipeline caused fuel shortages

SOURCE Ars Technica, Verge, New York Times. MOLLY NEWELL 5/17/21

“EO-Critical Software” Definition and Implementation

June 2021

- “EO-Critical Software” is defined as **any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:**
  - is designed to run with elevated privilege or manage privileges;
  - has direct or privileged access to networking or computing resources;
  - is designed to control access to data or operational technology;
  - performs a function critical to trust; or
  - operates outside of normal trust boundaries with privileged access.
- Definition **includes software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) purchased for, or deployed in, production systems and used for operational purposes**.

Initial phase will focus on **standalone, on-premises software** that has security-critical functions or poses similar significant potential for harm if compromised.

Subsequent phases may address software categories more broadly:

- software that controls access to data;
- cloud-based and hybrid software;
- software development tools;
- software components in boot-level firmware;
- software components in operational technology (OT); or
- embedded software and firmware.

EO Compliance Requirements & Int’l Regulation Correlations

Executive Order Compliance Requirements

Certificates of Compliance/Attestation ★

Require companies to provide attestations/certificates of product compliance re secure development practices & integrity and provenance of open-source software components - **India Telco; German IT, NIS 2**

Consumer IoT/Software Product Security Labeling ★

Requires NIST and FTC to identify IoT cybersecurity criteria for use in creation of a labeling program for IoT devices/ Consumer Software to reflect levels of security & testing – **Singapore, Australia, UK**

Software Bill of Materials ★

Requires companies to provide a comprehensive software bill of materials (SBOM) for in-scope products – **India Telco; China**

Software Development Environment Security

Requires companies to secure their software development environments (e.g., segregated build environments; MFA, data encryption)

Secure Software Development Practice

Establishes mandatory Secure Development Lifecycle requirements for in-scope products and public disclosure of select SDL practices (e.g., source code signing; vulnerability scanning)

Product Enablement

Critical features required in all products sold to federal government and covered critical infrastructure; for example, two-factor authentication

Vulnerability Disclosure ★

Requires companies to participate in a vulnerability disclosure program that includes reporting and disclosure requirements – **NIS 2; China, Australia**

Secure Component Sourcing/ Supply Chain ★

Requires companies to assess integrity and security of supplier software/components and their sourcing practices - **NIS 2, Australia, German IT, India Telco**

Threat Sharing ★

Requires (per contract) sharing of threat intel with government agency customers and collaboration in investigations to incident/potential incidents on FIS – **NIS 2**

Incident Response

Establishes notification obligations and timelines to report cyber incidents to the applicable agency and CISA – **NIS 2, Australia, China**

FAR/DFAR Contract Updates ★

Requires updates to FAR/DFAR regulations to codify security requirements for federal contracts

★ *Compliance requirements with international corollaries*

Emerging Global Security Laws

COMPUTER AND TECHNOLOGY SECTION

Supply Chain Assurance

- There is an increased focus on supply chain security around the globe. Governments are seeking increased transparency and assurance from vendors and service providers around information security

- These regulations are a reaction to (1) long-standing suspicions around Huawei in the 5G space and (2) the SolarWinds campaign of 2020
  - Executive Order on Cybersecurity 14028 (U.S.): will ultimately require vendors and service providers to the federal government to comply with requirements on secure software development and software bills of materials (SBOM), among other things.
  - IT Security Act 2.0 (Germany): Providers of “critical components” will need to provide “declarations of trustworthiness” to critical infrastructure operators and obtain certain infosec certifications, among other things.
  - Amendments to Unified Access Services License Agreement (UASL) for procurement of Telecom Equipment (India): will require OEMs providing equipment and/or software to telecom companies to provide detailed information about ownership and management, as well as hardware and software bills of materials.
  - Cybersecurity Law of the PRC: Cybersecurity product certification rules include SBOM-like requirements and supply chain risk management requirements.

Increased Direct Regulation

Initial signs indicate that multi-national companies will be subject to increased scrutiny in 2022:

- FTC Safeguards Rule (U.S., 2021): FTC's expanded rule includes explicit requirements around financial institution service provider supervision that may expose service providers to increased customer due diligence & more stringent security requirements.

- Network and Information Security Directive 2.0 (EU, Draft 2021): Proposes to implement a GDPR-like cybersecurity/product security regulation on important and critical entities operating in the EU, including manufacturers of computer, electronic and optical products and "ICT-service provider." This will subject large enterprises (i.e., > 250 employees, annual turnover of >€50 million) to more stringent government supervision and potential administrative fines of €10 million or up to 2% of total worldwide annual turnover, whichever is higher for cybersecurity-related violations and control failures.

- *Strengthening Australia's cyber security regulations and incentives*: Australia is currently contemplating establishment of voluntary and/or mandatory cyber/product security requirements for businesses operating in Australia (e.g. governance standards for large businesses, minimum standards for securing personal information, responsible disclosure policies, and possibly increased liability under the *Privacy Act* and/or Australian Consumer Law)

- Data Security Law & Personal Information Protection Law (China): Data protection and privacy law focused on increased security requirements around the collection and use of "Important Data" and associated restrictions on cross-boarder data transfer outside of Mainland China

China Data Protection Regulations & Cross-Border Data Transfer Restrictions

COMPUTER AND TECHNOLOGY SECTION

CHINA'S DATA PROTECTION & CROSS-BORDER DATA TRANSFER REGULATIONS

Cyber Security Law (CSL) (6/01/2017)

- Requires CIIOs to store personal information and "important data" in China or pass security assessment of CBDT

Data Security Law (DSL) (9/01/2021)

- Enacted to regulate data processing activities & improve data security
- Expands CSL data security requirements to all businesses that process "Important Data"
- Extends CBDT restrictions to Important Data

Personal Information Protection Law (PIPL) (11/01/2021)

- First comprehensive and dedicated personal information protection law in China
- Enacted to protect and regulate processing of personal information & address data processor's legal obligations
- Imposes severe control on personal information cross-border transfers.

Measures of Security Assessment on CBDT (Draft 11/01/2021)

- A matrix of laws, regulations and standards, attempting to build a CBDT mechanism in China.
- If made final, would apply to cross-border transfers of personal information and "important data".

Regional & Sectoral Regulations

- Sectoral requirements such as automotive measures.
- Clarifications, catalogs, and implementing rules are to be further developed and introduced.

China refers to mainland China for the purposes of these slides.
CIIO refers to critical information infrastructure operator.

CHINA DATA SECURITY LAW *(Effective 9/1/21)*

Key Provisions	Descriptions
Data Classification and Hierarchical Protection	• **Important Data**: Data if divulged, falsified or damaged, may directly affect national security, economic security, social stability, public health and security. Important data does not include personal information, core data and national secret information. ***Important Data is still undefined***; ***Identification Guidelines will be released by sector-specific supervisory regulators*** • **National Core Data:** Data related to national security, national economy, important parts of people's livelihood or major public interests
Cross-border Data Transfer (CBDT)	**For Important Data:** (a) CIIO: must store important data within China; to transfer this data abroad, Security Assesment must be undertaken by Cyberspace Administration of China; (b) Non-CIIO: CBDT restrictions are applied • Cross-border transfer of Important Data must secure regulator's assessment and approval prior to providing data to entities, foreign judicial systems or law enforcement
Data Security Management	• Establish end-to-end data security management system, data security and management body & data security incident management and report mechanism • Appointment of Data Security Officer (DSO). • May require localization of customer and employee data in China
Data Risk Assessment	• Regularly perform risk assessments over data handling activities and report to authorities. • Third-party CAC security assessments required for CBDT of Important Data

CHINA PERSONAL INFORMATION PROTECTION LAW (“PIPL”) (*Effective 11/1/2021*)

Applicable Data and Activity

- Personal Information: Various types of electronic or otherwise recorded information related to identified or identifiable natural persons, excluding anonymized information.
- Personal Information processing includes the collection, storage, use, processing, transmission, provision, disclosure and deletion of PI, etc.

Rules for Processing PI

- Similar framework to GDPR
- Establish seven legal basis of processing PI, in addition to consent
- Defines Sensitive PI & establishes more stringent rules on processing
- Specifies separate consent requirements for 5 scenarios of PI processing activities *(e.g. providing PI to the other processor, processing sensitive PI, PI cross-border transfer, public disclosure of PI, etc.)*

Rules for Cross-Border Transfer of PI

- Imposes significant controls/restrictions on PI cross-border transfer *(e.g. standard contract signoff, personal information protection certification, CAC security assessment, etc.)*
- Require PI data localization for CIIOs and large-scale PI transfers

Other Obligations of PI Processor

- Increases privacy compliance obligations of PI processors *(e.g., data incident notification and remediation measures, data protection impact assessments, etc.)*

CIIO refers to Critical Information Infrastructure Operator
CAC refers to Cyberspace Administration of China.

ADDITIONAL DSL & PIPL CROSS-BORDER DATA TRANSFER CONSIDERATIONS

CBDT SCENARIOS

Providing Data Outside of China

- Ex: Data transfer from China to the United States

Data Access by Foreign Entities

- Ex: Data physically located in China but accessed by entities in the United States

Limited Exclusions

- Ex: Data transferred from mainland China to Hong Kong, or US Embassy in China; publicly available information

APPLICABLE DATA

Personal Information

- Various types of electronic or otherwise recorded information related to identified or identifiable natural persons, excluding anonymized information

Important Data *(To be defined)*

- Data, if divulged, may directly affect national security, economic security, social stability and public health and security; does not include personal information, core data and national secret data
- Draft guidance suggests: economic operations data, population health data, gov't data, applications services data, network & information security data, etc.

General Data (*draft rules)

- Data that doesn't fall within one of the categories of personal information, important data,

APPLICABLE BUSINESSES

Critical Infrastructure Information Operators ("CIIOs")

- CIIOs are generally entities operating in the telecommunications, energy, transportation, water conservancy, finance, public service, national defense science and other important industries and fields.
- CIIOs must store personal information and important data within China. In order to transfer this data abroad, security assessments must be undertaken by CAC

Non-CIIOs

- CAC security assessment is required for cross-border transfers of important data by non-CIIOs (*draft rules)
- Transfers of personal information above certain threshold must undergo security assessment by CAC

KEY DRAFT RULES

Measures of Security Assessment on CBDT

- Apply to cross-border transfers of important data and personal information
- Before undertaking security assessment, a self-assessment must be conducted
- Approval is valid for 2 years. If there is a material change in the relevant circumstances, a new security assessment is required

Network Data Security Management Regulations (Draft 11.14.2021)

- Expands the application of CBDT requirements to "any data"
- If it were to come into force as presently drafted, could significantly add to compliance burden of multi-national companies

- **CAC** refers to Cyberspace Administration of China.
- **SA** refers to security assessment undertaken by CAC.
- **Important Data** definition and scope will be further defined through national, local and industrial rules, guidelines and catalogs.

Thank You!

Section Dues: $25.00

- Quarterly journal, *Circuits*
- Access to CTS App with Codes, Rules, and links to cases
- December CLE, Annual Meeting Track

COMPUTER AND TECHNOLOGY SECTION

Lavonne Burke Hopkins
Sr. Managing Legal Director, Security & Resiliency & IT
Dell Technologies, Inc.
Lavonne_Burke@Dell.com