UNNExT Workshop on the Legal Framework for Single Window

24-25 April 2012 – Seoul, Republic of Korea

DATA RETENTION, PRIVACY, DATA PROTECTION AND INFORMATION SECURITY

Professor William J. Luddy, Jr.

Legal Advisor, ASEAN Single Window Legal Working Group

Special Legal Counsel, World Customs Organization

Legal and Technical Aspects of Data Retention/Electronic Archiving

- Whether a Single Window is operating in the paper or electronic environments, the importance of keeping accurate records cannot be understated
- Data Retention or electronic archiving of documents and data is considered one important part of an overall robust information security program
- The information security protections in the NSW, such as authentication, access control and auditing, apply to both electronic data archiving (as well as to the archiving of paper documents)

Sources of Data Retention Requirements

- International Laws
- Regional Law (e.g., European Union)
- International Recommendations – *UN/CEFACT*
- Domestic Laws
- Domestic Regulations and Policies
- Agreements among government ministries
- Memoranda of Understanding (MOU) with Trade Participants

Legal Considerations for Determining Retention Periods

Data retention and destruction schedules should be based on:

- Purposes for which the documents were created
- Uses of the documents and information
- Appropriate policies to protect personally identifiable information (PII), trade sensitive, etc.
- Policy for what data is to be made publicly available
- Policy for what data is to be shared among government agencies

Electronic Archiving – Audit Logs and Backup Tapes

- Auditing should be established for the NSW to log specified trade transactions and those related to system and security issues
- Information security best practices require that audit logs are maintained online for an appropriate period of time such as 30 days so that transactions and events can be reconstructed readily if necessary
- Audit logs should be copied onto backup tapes periodically, such as daily or weekly
- The backup tapes are maintained offsite at a secure location; data for audits must be readily available

Security Considerations for Electronic Archiving

- Documents retained for a short period (six months), current secure technologies must be employed to preserve such electronic data
- Additional factors may need to be considered for documents maintained for longer periods (20 years)
- Current technology may become obsolete and electronic documents stored on "old" media may not be easily accessible
  - Media degrades
  - Support for older software versions
  - Encrypted data and encryption keys changing over time

Electronic Archiving and Data Destruction

- Information security protocols will need to be put in place to assure that the stored electronic documents are not compromised or changed
- Backup tapes must be stored in a secure location with stringent controls over their physical and electronic access
- There should be an affirmative obligation for data custodians to periodically review the data and information their custody to ensure that it is actually destroyed when the data retention period has expired
- Data must be destroyed by professionally acceptable means

Data/Information To Be Protected

- Customs and related government data
  - Such as trade-sensitive data
- Confidential business information
- Law enforcement data
- Information related to national security
- Personally identifiable information
- Others (based on legal requirements)

A Risk-based Framework of Security Controls

Operational controls are primarily implemented and executed by people (as opposed to systems)

Management controls focus on management of risk and the management of information system security

Technical controls are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system

Risk-Based Analysis

- Vulnerabilities
- Threats
- Risk Probabilities
- Countermeasures

Risk Analysis

- **Simply asks the questions:**
  1. **What is the *risk* that a particular *threat* will exploit a particular *vulnerability* that will result in damage?**
  2. **What are the legal implications if such damage does result?**

"Countermeasures"

- Minimizing the "high" risk areas
- Possible Technical Solutions:
  - Controlling Access to the NSW systems:
    - Identity Management Tools such as encryption, biometrics, tokens, access registry systems, etc.
    - Encrypting sensitive data/information
- Policy issue: How much is enough legally?

Privacy Considerations

- An important consideration in the information security equation
- Legal requirements for privacy (national legislation/regulations)
- Cross-border transmission of data
  - Are such exchanges legally authorized?
  - Trading partner country law?

Confidentiality, Integrity, Availability and Privacy

- Fundamental to protecting the information assets of government and private sector participants in the NSW:
- *Confidentiality* – Protection from Unauthorized Access and Disclosure
  - *Interception Threatens Confidentiality*
- *Integrity* – Protection from Alteration
  - Modification of Data Threatens Integrity
- *Availability* – Of Data and Service
  - Denial-of-Service Threatens Availability

Information Sharing and Secure Connectivity

- Details of information sharing agreements are set forth in:
  - Memoranda of Understanding (MOUs)
  - Interconnection Security Agreements (ISA)
- MOUs and ISAs can be developed for inter-Ministry use and inter-governmental arrangements between Single Windows
- Both technical and legal arrangements, including dispute resolution processes should be detailed in these documents

Recommendations

- The legal infrastructure for the Single Window in each country should include laws and/or implementing regulations and policies that:
  - Provide appropriate privacy and security protections for Personally Identifiable Information (PII), financial, confidential, trade secret, proprietary, and law enforcement data and information in the NSW
  - Ensure appropriate and effective approaches to data encryption and authentication when appropriate

Recommendations

- Conduct Privacy Impact Assessments (PIA) periodically for the NSW
- Consider developing a risk-based data breach notification policy

- Access and control procedures should be identified and included in regulations defining MOUs and ISAs
- Data Retention Policies should clearly define how they are to be implemented technically

- Questions?
- Comments?

Thank you!

Professor William J. Luddy, Jr.
Bill.Luddy@mac.com
William.Luddy@wcoomd.org