Legal Analysis for Implementation of Philippine National Single Window

Final Report

December 23, 2012

This Report was produced for review by the United States Agency for International Development. It was prepared by consultants for the USAID-funded ASEAN Single Window Project.
Legal Analysis for Implementation of Philippine National Single Window
Final Report

ASEAN SINGLE WINDOW PROJECT
CONTRACT NUMBER: 486-I-00-07-00008-00, TASK ORDER 3
NATHAN ASSOCIATES INC.
USAID/REGIONAL DEVELOPMENT MISSION FOR ASIA
DECEMBER 17, 2012
AUTHORS: DISINI & DISINI LAW OFFICE

DISCLAIMER:
The authors’ views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acronyms</td>
<td>v</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>ASW and PNSW Background</td>
<td>4</td>
</tr>
<tr>
<td>Report Purpose and Methodology</td>
<td>9</td>
</tr>
<tr>
<td>Current Functionalities of the PNSW</td>
<td>12</td>
</tr>
<tr>
<td>Legal Gap Analysis Report</td>
<td></td>
</tr>
<tr>
<td>A. Enabling the Single Window</td>
<td>17</td>
</tr>
<tr>
<td>B. Data Protection and Information Security</td>
<td>34</td>
</tr>
<tr>
<td>C. Access to and Sharing of NSW Data</td>
<td>50</td>
</tr>
<tr>
<td>D. Identification, Authentication and Authorization</td>
<td>68</td>
</tr>
<tr>
<td>E. Electronic Signatures and Certification Authorities – Mutual Recognition</td>
<td>72</td>
</tr>
<tr>
<td>F. Data Quality Regulations</td>
<td>78</td>
</tr>
<tr>
<td>G. Legal Liability and Dispute Resolution</td>
<td>80</td>
</tr>
<tr>
<td>H. Data Retention and Electronic Archiving</td>
<td>96</td>
</tr>
<tr>
<td>I. Intellectual Property Rights and Data Base Ownership</td>
<td>101</td>
</tr>
<tr>
<td>J. Competition Law Issues</td>
<td>107</td>
</tr>
<tr>
<td>K. Summary of Gaps and Recommendations by Priority</td>
<td>111</td>
</tr>
</tbody>
</table>
LIST OF ANNEXES

Annex A. Legal Issues Checklist

Annex B. PNSW Questionnaire

Annex C. Table of Questionnaire Status

Annex D. Workshop Attendance Sheet and Grouping

Annex E. Workshop Results: Comments on Recommendations

Annex F. Workshop Results: Sample Road Mapping

Annex G. Domain Areas/ Areas of Laws/ Sectors

Annex H. Matrix of Domestic Laws (Source Data)

Annex I. List of Relevant International Agreements and Guidelines for PNSW

Annex J. Copies of Domestic Laws, Rules and Regulations

Annex K. Copies of International Agreements
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAB</td>
<td>Authorized Agent Bank</td>
</tr>
<tr>
<td>ABC</td>
<td>Approved Budget for the Contract</td>
</tr>
<tr>
<td>ADR</td>
<td>Alternative Dispute Resolution</td>
</tr>
<tr>
<td>ADR Gov</td>
<td>Rules on Alternative Dispute Resolution for Disputes between National Government Agencies</td>
</tr>
<tr>
<td>AEC</td>
<td>ASEAN Economic Community</td>
</tr>
<tr>
<td>AFTA</td>
<td>ASEAN Free Trade Area</td>
</tr>
<tr>
<td>AGDB</td>
<td>Authorized Government Depository Bank</td>
</tr>
<tr>
<td>AHTN</td>
<td>ASEAN Harmonised Tariff Nomenclature</td>
</tr>
<tr>
<td>APEC</td>
<td>Asia-Pacific Economic Cooperation</td>
</tr>
<tr>
<td>APP</td>
<td>Annual Procurement Plan</td>
</tr>
<tr>
<td>ASEAN</td>
<td>Association of South East Asian Nations</td>
</tr>
<tr>
<td>ASW</td>
<td>ASEAN Single Window</td>
</tr>
<tr>
<td>ASYCUDA</td>
<td>Automated Systems for Customs Data</td>
</tr>
<tr>
<td>BAC</td>
<td>Bids and Awards Committee</td>
</tr>
<tr>
<td>BAI</td>
<td>Bureau of Animal Industry</td>
</tr>
<tr>
<td>BETP</td>
<td>Bureau of Export Trade Promotion</td>
</tr>
<tr>
<td>BFAD</td>
<td>Bureau of Food and Drugs</td>
</tr>
<tr>
<td>BFAR</td>
<td>Bureau of Fisheries and Aquatic Resources</td>
</tr>
<tr>
<td>BID</td>
<td>Bureau of Immigration and Deportation</td>
</tr>
<tr>
<td>BIR</td>
<td>Bureau of Internal Revenue</td>
</tr>
<tr>
<td>BIS</td>
<td>Bureau of Import Services</td>
</tr>
<tr>
<td>BLT</td>
<td>Build-Lease-and-Transfer</td>
</tr>
<tr>
<td>BOC</td>
<td>Bureau of Customs</td>
</tr>
<tr>
<td>BOI</td>
<td>Bureau of Investments</td>
</tr>
<tr>
<td>BOO</td>
<td>Build-Operate-and-Own</td>
</tr>
<tr>
<td>BOT</td>
<td>Build-Operate-and-Transfer</td>
</tr>
<tr>
<td>BPI</td>
<td>Bureau of Plants and Industry</td>
</tr>
<tr>
<td>BPS</td>
<td>Bureau of Product Standards</td>
</tr>
<tr>
<td>BQ</td>
<td>Bureau of Quarantine</td>
</tr>
<tr>
<td>BSP</td>
<td>Bangko Sentral ng Pilipinas</td>
</tr>
<tr>
<td>BT</td>
<td>Build-and-Transfer</td>
</tr>
<tr>
<td>BTO</td>
<td>Build-Transfer-and-Operate</td>
</tr>
<tr>
<td>BTr</td>
<td>Bureau of Treasury</td>
</tr>
<tr>
<td>CAAP</td>
<td>Civil Aviation Authority of the Philippines</td>
</tr>
<tr>
<td>CAMPI</td>
<td>Chamber of Automotive Manufacturers of the Philippines</td>
</tr>
<tr>
<td>CAs</td>
<td>Certification Authorities</td>
</tr>
<tr>
<td>CAS</td>
<td>Customs Accreditation Secretariat</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>CCN</td>
<td>Customs Client Number</td>
</tr>
<tr>
<td>CDEC</td>
<td>Cargo Data Exchange Center, Inc.</td>
</tr>
<tr>
<td>CEPT</td>
<td>Common Effective Preferential Tariff</td>
</tr>
<tr>
<td>CIDG</td>
<td>Criminal Investigation and Detection Group</td>
</tr>
<tr>
<td>CISA</td>
<td>Credit Information System Act</td>
</tr>
<tr>
<td>CPA</td>
<td>Cybercrime Prevention Act of 2012</td>
</tr>
<tr>
<td>CPRS</td>
<td>Client Profile Registration System</td>
</tr>
<tr>
<td>DA</td>
<td>Department of Agriculture</td>
</tr>
<tr>
<td>DAO</td>
<td>Department Administrative Order</td>
</tr>
<tr>
<td>DBP</td>
<td>Development Bank of the Philippines</td>
</tr>
<tr>
<td>DDB</td>
<td>Dangerous Drugs Board</td>
</tr>
<tr>
<td>DILG</td>
<td>Department of Interior and Local Government</td>
</tr>
<tr>
<td>DOF</td>
<td>Department of Finance</td>
</tr>
<tr>
<td>DOH</td>
<td>Department of Health</td>
</tr>
<tr>
<td>DOST</td>
<td>Department of Science and Technology</td>
</tr>
<tr>
<td>DOTC</td>
<td>Department of Transportation and Communication</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Privacy Act of 2012</td>
</tr>
<tr>
<td>DST</td>
<td>Documentary Stamp Tax</td>
</tr>
<tr>
<td>DTI</td>
<td>Department of Trade and Industry</td>
</tr>
<tr>
<td>ECA</td>
<td>Electronic Commerce Act</td>
</tr>
<tr>
<td>EEC</td>
<td>Entry Encoding Center</td>
</tr>
<tr>
<td>EFPS</td>
<td>Electronic Filing and Payment System</td>
</tr>
<tr>
<td>EIPS</td>
<td>Electronic Import Permit System</td>
</tr>
<tr>
<td>EMB</td>
<td>Environment Management Bureau</td>
</tr>
<tr>
<td>EO</td>
<td>Executive Order</td>
</tr>
<tr>
<td>EPCS</td>
<td>Electronic Payment and Collection System</td>
</tr>
<tr>
<td>EPGP</td>
<td>Electronic Payment Gateway Provider</td>
</tr>
<tr>
<td>ETA</td>
<td>Electronic Transactions Act</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>E2m</td>
<td>e2m Customs Project</td>
</tr>
<tr>
<td>FDA</td>
<td>Food and Drug Administration</td>
</tr>
<tr>
<td>FEO</td>
<td>Firearms and Explosives Office</td>
</tr>
<tr>
<td>FIDA</td>
<td>Fiber Industry Development Administration</td>
</tr>
<tr>
<td>FMB</td>
<td>Forest Management Bureau</td>
</tr>
<tr>
<td>FPA</td>
<td>Fertilizer and Pesticides Authority</td>
</tr>
<tr>
<td>GAA</td>
<td>General Appropriations Act</td>
</tr>
<tr>
<td>GATT</td>
<td>General Agreement on Tariffs and Trade</td>
</tr>
<tr>
<td>GEPCSET</td>
<td>Government Electronic Payment and Collection System Evaluation Team</td>
</tr>
<tr>
<td>GISP</td>
<td>Government Information Systems Plan</td>
</tr>
<tr>
<td>GSIS</td>
<td>Government Service Insurance System</td>
</tr>
<tr>
<td>HDMF</td>
<td>Home Development Mutual Fund (Pag-IBIG)</td>
</tr>
<tr>
<td>IC</td>
<td>Insurance Commission</td>
</tr>
</tbody>
</table>
ICTO  Information and Communications Technology Office
IP    Intellectual Property
IPO   Intellectual Property Office
IRR   Implementing Rules and Regulations
IRRES Implementing Rules and Regulations on Electronic Signatures
ISMS  Philippine National Standards on Information Security Management System
ISO   International Organization for Standardization
JDAO  Joint Department Administrative Order
LBP   Land Bank of the Philippines
LTO   Land Transportation Office
MARINA Maritime Industry Authority
MB    Monetary Board
MISTG Management Information Systems Technology Group
MOA  Memorandum of Agreement
MVPMAP Motor Vehicle Parts Manufacturers Association of the Philippines
NEDA  National Economic and Development Authority
NFA   National Food Authority
NICA  National Intelligence Coordinating Agency
NMIS  National Meat Inspection Service
NPC   National Privacy Commission
NSW   National Single Window
NTC   National Telecommunications Commission
OECD  Organization for Economic Cooperation and Development
OMB  Optical Media Board
PDEA  Philippine Drug Enforcement Agency
PEZA  Philippine Economic Zone Authority
PHIC  Philippine Health Insurance Corporation (PhilHealth)
PHILCOA Philippine Coconut Authority
PHILPASS Philippine Payments and Settlement System
PNP   Philippine National Police
PNRI  Philippine Nuclear Research Institute
PNSW  Philippines National Single Window
PNSW-SC Philippine National Single Window – Steering Committee
PNSW-TWG Philippine National Single Window – Technical Working Group
POD  Philippine Ozone Desk
PPA  Philippine Ports Authority
PSB  Philippine Shippers’ Bureau
PVB  Philippine Veterans Bank
RA   Republic Act
RAC  Revised Administrative Code
RAI  Records of Actual Inspection
REE  Rules on Electronic Evidence
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROC</td>
<td>Rules of Court</td>
</tr>
<tr>
<td>RPC</td>
<td>Revised Penal Code</td>
</tr>
<tr>
<td>RR</td>
<td>Revenue Regulation</td>
</tr>
<tr>
<td>SAD</td>
<td>Single Administrative Document</td>
</tr>
<tr>
<td>SEIP</td>
<td>Semiconductor and Electronic Industries of the Philippines</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identification Module</td>
</tr>
<tr>
<td>SRA</td>
<td>Sugar Regulatory Administration</td>
</tr>
<tr>
<td>TC</td>
<td>Tariff Commission</td>
</tr>
<tr>
<td>TCC</td>
<td>Tariff and Customs Code</td>
</tr>
<tr>
<td>TTA</td>
<td>Technology Transfer Arrangements</td>
</tr>
<tr>
<td>UCPB</td>
<td>United Coconut Planters Bank</td>
</tr>
<tr>
<td>UMID</td>
<td>Unified Multi-Purpose ID</td>
</tr>
<tr>
<td>UNCEFACT</td>
<td>United Nations Center for Trade Facilitation and Electronic Business</td>
</tr>
<tr>
<td>UNCTAD</td>
<td>United Nations Conference on Trade and Development</td>
</tr>
<tr>
<td>VAS</td>
<td>Value Added Service Provider</td>
</tr>
<tr>
<td>VASP</td>
<td>Value Added Service Provider</td>
</tr>
<tr>
<td>WCO</td>
<td>World Customs Organization</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organization</td>
</tr>
</tbody>
</table>
Executive Summary

This Report is a legal analysis dealing with the various issues involved in the implementation of the Philippine National Single Window (PNSW). It also addresses the legal interoperability between the PNSW and other ASEAN Member State’s National Single Windows (NSWs) and the ASEAN Single Window (ASW). The various areas investigated are as follows:

Enabling the Single Window. The Philippines is currently developing its implementation of a PNSW under the auspices of Executive Order 482. This initiative is supported by a legal framework under the E-Commerce Act (ECA) that expressly authorizes electronic transactions, recognizes the validity of electronic documents, and provides procedures for admission of electronic evidence in evidentiary hearings. Nevertheless, despite textual commitments to a functional equivalent approach, the law and its subsequent judicial interpretations make the parity between electronic and paper documents difficult to implement in practice. Although the passage of Executive Order 482 provided the basic framework for cooperation and coordination between participating government agencies, a stronger commitment to the single window initiative is needed. Provisions for funding of the operation and maintenance of the system, is also essential to make PNSW more viable in the long term.

Data Protection and Privacy. Philippine law primarily frames data protection in terms of providing penal sanctions for performing prohibited acts on data and data systems. Recently, the Philippine legislature enacted the Data Privacy Act of 2012 (DPA) covering the collection of personal information by both the government and the private sectors. The law includes notice, consent and data breach notification requirements for data controllers and data processors, and outlines the corresponding rights of data subjects. The law also establishes a National Privacy Commission (NPC) to administer the law and monitor compliance.

Although the current PNSW implementation utilizes standard security measures, no legal or administrative issuance provides for standards and best practices at a system-wide level that may be applicable to all participating government agencies. Nevertheless, in the absence of detailed legal proscriptions, the said agencies may adopt documented international standards on establishing and maintaining an information security management system.

Access to and Sharing of NSW Data. Other than separate administrative issuances and/or agreements between some government agencies, there appears to be no existing formal law that specifically mandates the allowable sharing of information across all government agencies. The current legal framework for access and sharing of data is generally based on provisions in the 1987 Philippine Constitution (Philippine Constitution) relating to private and public information, legal requirements for the adoption of a unified ID system, and the DPA. The Memorandum of Agreement on the Implementation of the Philippine National Single Window (PNSW MOA) signed on
February 10, 2012 among the participating government agencies recognized the need to come up with clear rules and regulations on access and sharing of information within the PNSW. Such rules and regulations however should carefully consider the provisions of the laws mentioned.

Identification, Authorization and Authentication. The components that form the PNSW’s first line of security consists of technological methods for (a) identifying and authenticating legitimate users; and (b) authorizing operations and transactions based on these credentials. However, PNSW’s registration and accreditation component is not elaborated in a separate policy or integrated into an overall security management plan. Participating government agencies operate on a sectoral or “silo” approach, where accreditation mechanisms arise on an application-by-application basis. Provisions for cross-border authentication should be put in place and implemented either through multilateral arrangements or a standard for terms of use that will bind users and NSWs.

Electronic Signatures and Certification Authorities. Philippine law recognizes electronic signatures with reference to the functional equivalence approach, and premises this recognition upon restrictive requirements such as proof of integrity and reliability of the transaction system. Although independent proof of the genuineness or the integrity or reliability of the electronic document is not required when it comes to the authentication of digital signatures, yet, applicable laws and administrative issuances reveal that the only digital signatures that are recognized are those that arise from an asymmetric cryptographic system with a public key infrastructure. This effectively limits the technological neutrality of the country’s legal framework on digital signatures.

Data Quality. There is currently no overarching data quality policy for the PNSW, as data quality regulations occur in “silos” limited to a particular agency or a specific transaction. Although the DPA provides a limited quality maintenance mechanism that allows users to dispute and correct inaccurate or erroneous records, there is no regulation covering an inter-agency, systematic approach to audits or incident response and management, in cases when data quality is flagged.

Legal Liability and Dispute Resolution. Dispute resolution mechanisms under Philippine law are classified into judicial or alternative modes of dispute resolution. At present there are no rules on Alternative Dispute Resolution (ADR) for NSW transactions. However, for disputes arising under the Agreement to Establish and Implement the ASEAN Single Window (ASW Agreement), the ASEAN Protocol on Enhanced Dispute Settlement Mechanism shall apply. Also, since Philippine law adheres to the spiritual system of contracts, provisions for arbitration may be expressly provided in model consortium agreements and end-user agreements for NSW users, as well as, in agreements between and among NSWs.

Data Retention and Electronic Archiving. Essentially, the pertinent provisions of the DPA, ECA and Executive Order No. 265 establishing the Government Information Systems Plan (“GISP”) form the legal framework for data retention and archiving. Some government agencies also have their own rules on data retention and archiving,
particularly covering transactions governed by their agencies. For the purpose of the PNSW, it would be best to craft a uniform set of rules on archiving and record keeping across all government agencies, which rules should follow standard procedures and comply with international standards. As to the evidentiary value of stored data, there is as of yet no law or regulation that would ensure that data utilized and exchanged by NSWs and the ASW will be retained to meet judicial and evidentiary requirements in the event of disputes.

**Intellectual Property Rights and Data Base Ownership.** The Philippine Constitution mandates the protection of intellectual property, which policy is implemented by the Intellectual Property Code (IP Code). The Philippines is also a member - signatory to most major international agreements and treaties respecting intellectual property rights. In addition, the Supreme Court of the Philippines has issued special rules of procedure in intellectual property cases, and has designated special courts that decide cases on intellectual property disputes. Similarly, the National Bureau of Investigation (NBI) and Criminal Investigation and Detection Group (CIDG) have divisions specifically dedicated to the enforcement of intellectual property rights. The Philippines also has an Optical Media Board (OMB) created for the purpose of preventing optical media piracy. However, as for the protection of intellectual property rights that may exist over data or information gathered in cross-border transactions by the NSWs and the ASW, it is submitted that since the data received are mostly facts (not in the nature of literary or derivatives thereof), the same are not deemed to be covered by copyright protection laws in the Philippines.

**Competition Law Issues.** Competition is not regulated in the Philippines, and it is only in some industries that government exercises some form of control. Nevertheless, the issuance of Executive Order No. 45 designating the Department of Justice (DOJ) as the Competition Authority is considered a step towards promoting competition and a level playing field in domestic and international trade. However, apart from the general anti-trust policy embodied in the Philippine Constitution, no specific anti-trust law has been passed by the Legislature.
ASW and PNSW Background

The ASEAN Single Window (ASW)

From its inception on August 8, 1967, Member States of the Association of Southeast Asian Nations (ASEAN), namely: Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam, have worked together and have consistently moved towards several common objectives, which include safeguarding their political stability, resolving intra-regional differences and promoting social and cultural development. Among these objectives and probably the most crucial of all, is the promotion of economic development among Member States.

To pursue economic development in the region, several cooperative agreements were adopted by the Member States, which led to the establishment of the ASEAN Free Trade Area (AFTA) and the Common Effective Preferential Tariff (CEPT) scheme. These cooperative measures aimed to eliminate or at least reduce the tariff rates levied on products traded within the region, in order to bring about a smooth cross-border flow of goods and increase the region’s competitive advantage in the world market.

Consistent with this objective, the ASEAN Agreement on Customs mandated the creation of a simplified, efficient and harmonized, trade and customs rules of procedures, and the application of consistent, transparent and fair customs laws and regulations among the Member States, geared towards the efficient and expeditious clearance of products traded within the region. Accordingly, on January 1, 2002, the Member States adopted the Protocol Governing the Implementation of the ASEAN Harmonised Tariff Nomenclature (AHTN Protocol) that established an 8-digit commodity tariff nomenclature towards a uniform classification of goods traded within the region.

As the need to minimize the incidence and complexity of import and export formalities, and the need to decrease and simplify import and export documentation requirements were being recognized, Member States were directed to adopt international best practices in trade facilitation, such as the use of a Single Window. It was the Declaration of ASEAN Concord II signed on October 7, 2003, where the idea of a Single Window received the highest level of endorsement among the Member States. The Concord

---

1 The ASEAN Declaration (Bangkok Declaration), 8 August 1967.
2 Agreement on the Common Effective Preferential Tariff (CEPT) Scheme for the ASEAN Free Trade Area, 28 January 1992.
3 The ASEAN Agreement on Customs was executed on March 1, 1997. Before this, there was also the ASEAN Customs Code of Conduct that was first signed on March 18, 1983 (which was later amended sometime 1995), that also committed to facilitate the simplification and harmonization of customs procedures.
4 ASEAN Agreement on Customs, 1 March 1997, arts. 1, 2 & 6.
5 Protocol Governing the Implementation of the ASEAN Harmonised Tariff Nomenclature, 1 January 2002, art. 3.
6 General Agreement on Tariffs and Trade 1994 (Fees and Formalities Connected with Importation and Exportation), 15 April 1994, art. VIII.
authorised the creation of an ASEAN Economic Community (AEC) whose end-goal by Year 2020 is to create a stable, prosperous and highly competitive ASEAN economic region in which there is a free flow of goods, services, investment, and a freer flow of capital,\(^7\) that is economically integrated with effective facilitation for trade and investment.\(^8\) This eventually paved the way for the ASW that envisioned the electronic processing of trade documents through a Single Window, at both the regional and national levels. Consequently, on November 29, 2004, the **ASEAN Framework Agreement for the Integration of Priority Sectors** (Framework Agreement) was signed. The Framework Agreement identified the development of the Single Window approach as one of the measures to be implemented in respect of the priority sectors.\(^9\)

On December 9, 2005, the Member States\(^10\) signed the ASW Agreement. The objective of the ASW Agreement is to provide a legal framework to establish and implement the ASW, where the NSWs of Member States can operate and integrate.\(^11\) Article 5, paragraph 1 of the ASW Agreement states that: “Member States shall develop and implement their National Single Windows in a timely manner for the establishment of the ASEAN Single Window.” Different deadlines were set for the Member States to operationalize their NSWs. For Brunei Darussalam, Indonesia, Malaysia, Thailand, Singapore and the Philippines, the deadline is no later than 2008, and no later than 2012 for Cambodia, Lao PDR, Myanmar and Vietnam.\(^12\)

The **Protocol to Establish and Implement the ASEAN Single Window** (ASW Protocol) was signed by the Member States on December 20, 2006, as directed under Section 6 of the ASW Agreement. Among the objectives of the ASW Protocol was to provide a legal and technical framework to establish and implement the ASW and the NSWs, towards the establishment of the AEC.\(^13\) The ASW Protocol defined ASW to be “the environment where the NSWs of Member States operate and integrate” \(^14\) and defined NSW to be “the system which enables: (a) a single submission of data and information (b) a single and synchronous processing of data and information; and, (c) a single decision-making for customs release and clearance of cargo.\(^15\) A system for a single decision-making was uniformly interpreted under the ASW Protocol to be a single point of decision for the release of cargoes by the Customs on the basis of decisions, if required, taken by line ministries and agencies and communicated in a timely manner to

---

\(^7\) Declaration of ASEAN Concord II, 7 October 2003, Section B.


\(^9\) **ASEAN Framework Agreement for the Integration of Priority Sectors**, 29 November 2004, as amended on 8 December 2006, art. 8(f).

\(^10\) The Republic of the Philippines was among the Member States who signed the ASW Agreement.

\(^11\) Agreement to Establish and Implement the ASEAN Single Window, 9 December 2005, part 1, art. 1 and part II, art. 3.

\(^12\) Ibid., part III, art. 5.

\(^13\) Protocol to Establish and Implement the ASEAN Single Window (ASW), December 20, 2006, art. 2.

\(^14\) Ibid., art. 1(1a).

\(^15\) Ibid., art. 1(1b).
the Customs. The ASW Protocol also came up with the *ASW Action Plan*, which scheduled the activities for the ASW implementation, and the *ASW Technical Guide*, which is a “compilation of relevant internationally accepted standards, procedures, documents, glossary, technical details and formalities for the effective implementation of the ASW, to be adopted as deemed appropriate by Member States”.

During the 8th Meeting of the Working Group on Legal and Regulatory Matters for the ASW, held in Bangkok, Thailand, the Member States agreed that in the implementation of the ASW Pilot Project, the “federated/regional approach” shall be observed, which basically restricts the ASW from maintaining or retaining any trade related customs data or information that may be transmitted from or to the ASW. Such data may be lodged with and maintained in the respective NSWs of the Member States and the ASW just keeps a record of their transmission, which record does not include the content of the data or information transmitted.

**The Philippine National Single Window (PNSW)**

Upon the adoption of the ASW Agreement by the Philippines and other Member States on December 9, 2005, several Inter-Agency Task Force meetings were held for the purpose of coming up with a uniform interpretation of the ASW, and to affirm that the customs authorities of each of the Member States should be the final and single decision-maker on cargo clearance and release. The understanding among the Member States is that the NSW system that each will develop should enable a single submission of data and information that is synchronously processed, resulting in a single point of decision for release of cargoes by customs, based on decisions made by other departments and agencies of government and communicated in a timely manner to customs.

Note however that even before the ASW Agreement was signed by the Member States, the Philippines already volunteered to be the pilot country for the implementation of the NSW for Cargo Clearance, during the 3rd Inter-Agency Task Force Meeting on ASW held in Manila sometime April 2005. This paved the way for the passage of EO 482 on

---

16 Protocol to Establish and Implement the ASEAN Single Window (ASW), December 20, 2006, art. 1(1b).
17 Ibid., art. 1(3) & (4).
18 On August 24-26, 2009, the Member States met and agreed to a draft of the Memorandum of Understanding on the Implementation of the ASEAN Single Window Pilot Project, which directed the implementation of the ASW Pilot Project with test data and information coming from the Member States’ respective NSWs.
20 Ibid., art. I (3).
22 Ibid.
23 Ibid.
December 27, 2005, Creating the National Single Window Task Force for Cargo Clearance (EO 482).

Under EO 482, a PNSW Task Force for Cargo Clearance (PNSW Task Force) was created, composed of a Steering Committee (PNSW-SC) and a Technical Working Group (PNSW-TWG). The PNSW-SC was mainly responsible for setting the policy guidelines for the creation and operation of the NSW and the ASW, and ensuring their efficient implementation. The PNSW-TWG was responsible for implementing the policies and directives of the PNSW-SC, identifying a common set of data, information and processes to be standardized and integrated, and at the same time ensuring data integrity and security, and delineating the roles and responsibilities of each government agency that should participate in the PNSW project. The initial plan of the PNSW-SC was to implement a completely internet-based network for Single Window partners. Involved in the PNSW project are no less than 40 participating government agencies, 30 of which issue cargo permits and clearances, and 10 of which are monitoring and accrediting agencies.

To pursue inter-agency cooperation, the Bureau of Customs (BOC) signed several agreements with participating government agencies that were key to the PNSW. Examples of such agreements were those signed on October 2006 among the BOC, Philippine National Police (PNP), Philippine Economic Zone Authority (PEZA) and the Semiconductor and Electronic Industries of the Philippines (SEIP) in line with the objectives of the NSW, and the agreement signed by the Department of Agriculture (DA) with the Secretary of Finance to pilot a NSW activity that establishes an inter-agency linkage between the BOC and the attached agencies of the DA. Under the latter agreement, the DA agencies shall exchange import and export clearance information with the BOC, and the latter shall provide hardware, connectivity and software.

---

24 The PNSW-SC is composed of the Secretary of Finance as Chairman, the Secretaries of the DTI, DA, DOTC, DILG, DOH, the Governor of the BSP and the Director General of the NEDA, as members.
25 EO 482, secs 1, 2 & 4.
26 The PNSW-TWG is composed of the Commissioner of the BOC as Chairman, and the Heads of the BIR, ICTO, TC, PPA, BPI, BQ, FDA, BAI, BIS, LTO, IC, PEZA, and the Mabuhay and Non-Mabuhay Lane of the DOF.
27 EO 482, sec. 4.
28 Alex V., “Enabling the PNSW for Cargo Clearance” (presented during the Orientation and Workshop for the Philippine National Single Window: Proceedings, 20 August 2007).
30 FMB, MIA, NFA, NMIS, NTC, OMB, PHILCOA, PDEA, PEZA, PNP, PNRI, POD and the SRA.
Directives to facilitate the implementation of the PNSW have also been issued by some of the participating government agencies. The DA issued the Revised Guidelines Governing the Importation of Agricultural and Fishery Commodities into the Philippines (Sanitary and Phyto-Sanitary [SPS] Regulations) where it recognized the implementation of the PNSW for electronic processing of trade documents. The Sugar Regulatory Administration (SRA), for its part, issued Circular Letter No. 8, Series of 2010, to effect the implementation of electronic filing with the PNSW system as the sole method of applying for a clearance and release of imported sugar. The Circular gave detailed instructions to importers and brokers and the personnel of SRA on the application process for the Clearance for Release of Imported Sugar, as implemented under the PNSW. The ultimate objective is to phase out the use of paper permits and clearances in the processing of imports and exports, as part of the BOC clearance procedure, and to completely disallow the use of hard copy/paper permits and clearances.  

The National Food Authority (NFA) also issued their General Guidelines in the Importation of Well-Milled Rice” (NFA Guidelines) on January 5, 2011, where it directed that all import permits to all interested importers under the program shall be through the use of the PNSW. Regional implementation of the PNSW has likewise started since August 2010 to seven (7) pilot agencies with regional offices, such as the Bureau of Quarantine (BQ), Bureau of Product Standards (BPS), Fertilizer and Pesticide Authority (FPA), Food and Drug Administration (FDA), National Meat Inspection Service (NMIS) and the National Telecommunications Center (NTC).  

On February 10, 2012, almost all participating government agencies formally signified their cooperation towards the successful implementation of the PNSW by signing the PNSW MOA. Under the PNSW MOA, the participating government agencies agreed to provide technical and legal personnel and establish information sharing procedures between and among themselves in order to carry out the objectives of the PNSW.

---

34 Bureau of Customs Letter addressed to the Administrator of the SRA, dated November 5, 2010.
36 It was only the BIR that did not sign the PNSW MOA.
37 Memorandum of Agreement on the Implementation of the Philippine National Single Window, (February 12, 2012), arts. III and VII.
Purpose and Methodology

Purpose of the Report

The purpose of this Report is to assist the Philippines in preparing a comprehensive legal analysis for the implementation of the ASW, the PNSW and its components. The Report provides legal analysis to aid the development of the PNSW and to prepare for its role within the ASW. The Report identifies legal gaps in domestic laws that would create barriers to:

(a) The implementation of the PNSW;

(b) The cross-border legal interoperability between PNSW and other ASEAN Member States’ NSWs; and

(c) The legal interoperability of the PNSW or the components of the PNSW and non-government entities that will participate in the PNSW and electronic commerce domestic and cross-border trading transactions.

Methodology

The Report is a product of in-depth research and analysis of Philippine domestic laws, regulations, decrees, orders, guidelines, policies and judicial decisions related to the current state and the legal issues related to the implementation of the PNSW. It identifies gaps in the domestic legal framework that need to be addressed for the full implementation of the PNSW and its cross-border interoperability in an electronic environment. The obligations of the Philippines under related international agreements and treaties on the ASW are likewise covered in the Report.

The Report covers the specific topics and issues under the Basic Gap Analysis Legal Checklist (Annex “A”), and such other national laws that were not originally included in the list, but which may have an impact on and/or relationship to the PNSW and the ASW.

A standard legal research methodology and approach typical of a high-level research effort was employed, using the following legal materials:

• Primary legal sources that represent the research focus were used. These included legal instruments such as enacted legislation, statutes and laws, decrees and executive orders, circulars and the like having the force of national law, formally adopted and promulgated regulations and rulings, judicial and administrative decisions, etc.
• Secondary legal sources (e.g., legislative history, ministry, administrative and executive reports) were reviewed and included to provide background and interpretations of the primary legal materials.

• Other legal materials relevant to the development of the PNSW and related electronic commerce legal framework developments in national law (e.g., law review articles, conference reports and international commentary) were examined and included as well.

The Report systematically responds to the questions in Annex “A” and expanded the field of inquiry to relevant areas which may have not been considered – such as nuances in local law that may have an impact on other areas of inquiry. The legal gaps are identified at the end of each topic, as well as recommendations that range from administrative stop-gap measures (that allow the PNSW to proceed with minimal effort while longer-term regulations are being worked out) to full blown legislation.

Inception Report

As agreed in the Terms of Reference, an Inception Report was presented to the BOC on July 16, 2012. The Inception Report served as the preliminary document that introduced the Authors, their backgrounds, the coverage of the Report and the research methodology to be adopted.

Agency Meeting and Questionnaire

On August 2, 2012, the Authors attended the Agency Coordination and TWG Meeting No. 6 held in the BOC, where they were formally introduced to some of the participating government agencies that were in attendance. During the said meeting, Crown Agents, for Overseas Government and Administrations, Ltd. (Crown Agents), the consultant and systems integrator of PNSW, gave its status update and presented pending matters and discussed resulting issues with the participating government agencies.

The Authors subsequently created a Questionnaire (Annex “B”), and with the help of the BOC and Crown Agents, it was successfully sent to forty-three (43) participating government agencies, by email and/or fax. The said agencies were requested to answer very specific questions on the different topics of the research, and shared their valuable inputs and feedback. As of the time of writing of this Report, thirty-four (34) of the participating government agencies have confirmed receipt of the Questionnaire and seventeen (17)\footnote{These agencies are as follows: BAI, BOC, BIR, BPI, Crown Agents, DDB, FPA, FIDA, IC, NFA, PDEA, BSP, Philippine Ozone Desk, PEZA, BQ, BIS and FDA.} of these agencies have submitted their responses.
Interim Report and Presentation

The Interim Report was formally presented to the BOC and the other participating agencies, including other stakeholders, on October 2, 2012 at the Heritage Hotel Manila. It was a whole day presentation where the Authors discussed their findings and recommendations in relation to the components of the Report, and where the participants had the opportunity to ask questions and clarify issues in relation to the Report and the operations of the PNSW. The Authors were also able to get valuable inputs from the stakeholders, which inputs were considered and incorporated into the Draft Final Report.

Draft Final Report and Workshop

The Draft Final Report was formally submitted on December 3, 2012, during the workshop that was conducted by the Authors in Diamond Hotel, Manila. The Authors focused on the presentation of their Recommendations, which were classified into High, Medium and Low Priority. After the presentation, the participants had the opportunity to ask questions on the recommendations as presented by the Authors, after which they were divided into three (3) general groups, High, Medium and Low Priority. Each group had its own representative from the Authors as facilitator.

During the first part of the workshop, the groups were instructed to review and discuss the recommendations for their particular group and consolidate their comments, modifications and amendments to the said recommendations. The purpose of the exercise was to obtain the specific requirements, concerns or issues that are unique and peculiar to the agencies represented, that may have an impact on the recommendations. On the second part of the workshop, the Authors instructed the groups to pick out one recommendation for which they were asked to chart a road map. The task consisted of mapping out the particular steps that need to be taken to implement the recommendation, identifying the point person or point agency that will initiate the steps, and indicating the timetable for execution. The first group was asked to pick a recommendation that required the enactment of a law. The second group picked one that required the passage of implementing rules and regulations concerning technology matters, and the last group worked on the recommendation that called for the enactment of rules of procedure in the Supreme Court. The exercise was meant to guide the participants on how to proceed with the implementation of the recommendations formulated by the Authors, with the hope that they can simulate the process within their respective agencies.

39 A fourth group was created specifically for recommendations that concerned the newly enacted Data Privacy Act (DPA). However, because the group participants were not yet familiar with the provisions of the DPA, the group facilitator just explained the salient features of the DPA to the members and discussed them in relation to the recommendations suggested by the Authors.

40 These valuable feedback and input from the participants were considered and incorporated by the Authors in this Final Report.
Current Functionalities of the PNSW

1. The PNSW functions as a centralized facility where registered traders, who are accredited by the participating government agencies with which they wish to transact, are given access to the system through the Internet. The permit or clearance applications submitted by the trader through the system are routed automatically to the participating government agencies where they are processed and approved. Information of the approval is sent back to the system for viewing and tagging by the BOC, so it can thereafter process the release of the cargo within its own operational system.

2. The PNSW Project was awarded in October 2009, after public bidding, to Crown Agents, based on its “TRIPS Single Window” product. Crown Agents started the configuration of the PNSW in November 2009, and in a month’s time, ten (10) agencies were already configured for pilot running, using the one priority application form that was initially selected for permit to import. It has been reported that the PNSW is currently used in thirty (30) government agencies, seventy (70) regional offices, and ten (10) monitoring and accrediting government agencies.

3. The PNSW makes possible the electronic submission of more than seventy (70) applications for cargo import and export permits and clearances using a single internet-based interface. It enables notification via email of the status of the application, and allows the trader to check the status in the PNSW dashboard, where other information on the application is also accessible. Security of submitted data is enabled using digital signatures on PDF documents; and the required supporting documents to the applications can be scanned and attached electronically.

4. For payment of fees, the traders manually paid directly to the cashiers of the participating government agencies. The said agencies accordingly received payment, issued the manual invoice and official receipt, and updated the status

---

41 UN Economic Commission for Europe, Geneva. Single Window Case Study Template (Philippines).
42 Ibid.
43 Ibid
44 Ibid.
46 Information found in the Department of Agriculture website.
47 UN Economic Commission for Europe, Geneva. Single Window Case Study Template (Philippines).
48 Ibid.
of the application in the PNSW system by indicating that the application fee for
the permit or clearance had been paid, and proceeded to approve the same.49

5. At present, the system workflow of the PNSW has already been enabled with an
online payment system serviced by Bancnet. The interface for online payment
was completed successfully and two government agencies namely, NTC and
SRA already launched the system on November 29, 2012. Full implementation of
the online payment system is expected by first week of January 2012. 50

6. For purposes of transparency, an audit trail function is included in the system that
records any changes or actions of the participating government agencies with
respect to the application.

7. An electronic-to-mobile communications system for all participating government
agencies dealing with the BOC was also made possible through a wireless
solution composed of a cellular phone Subscriber Identification Module (SIM) that
uses Short Message Service (SMS) and web-based technology.51 This allows
BOC employees to monitor and do their transactions via mobile phone, and
allows the said agencies to use SMS to check the authenticity and verify, on real-
time, the licenses and permits issued by the other agencies.52

8. Note, however, that before the implementation of the PNSW, the BOC already
used, and continues to use, the Automated Systems for Customs Data
(ASYCUDA), a project of the United Nations Conference on Trade and
Development (UNCTAD),53 more commonly referred to within the BOC as its
e2m Customs Project (e2m).54

9. The e2m is composed of a back-end system operated by BOC and a front-end
web-based interface developed and operated by Value-Added Service Providers
(VASPs). The e2m facilitates the processing of import and export declarations
and clearances, by requiring traders, acting through customs brokers, to register
through its Client Profile Registration System (CPRS).55 The information for
accreditation that was previously lodged with Entry Encoding Centers (EECs) is
now lodged with the VASPs, that validate the information electronically and
stores it in a central database.

49 Reported by Ms. Sally S. Alvareda of Crown Agents during the Inception Meeting at the Bureau of
Customs on 16 July 2012.
50 As reported by Sally Alvareda of Crown Agents.
51 Ibid.
52 Ibid.
54 The e2m Customs Project was launched in January 2005.
10. The e2m made possible online submission of declarations with automatic advice on the status of such declarations. It established links with relevant government agencies and provided online resource access through BOC’s website, issuances, processes, policies, guidelines and other related information.

11. Although traders who have been registered in the e2m before April 1, 2010 have been automatically registered in the PNSW system, there is, as of yet, no link between the BOC’s e2m and the PNSW. Currently, information on the e2m is manually entered by the BOC into the PNSW, while some PNSW data are entered into the e2m through the traders’ customs brokers.

12. In Phase 1 of its implementation of the PNSW, Crown Agents integrated the old manual system of the participating government agencies with as little change as possible to the said agencies’ existing procedures. This was intended to ease the transition into the new online PNSW system and to accommodate the familiarity of the traders, as well as that of the public officers, with the standard application procedures of the agencies concerned. For instance, the same exact paper application forms used by the participating government agencies for its permits and licenses were simply converted to PDF format and immediately uploaded into the PNSW site.

13. Each application form submitted under the PNSW is provided with a unique transaction reference number and the status of each application and other related information is viewed using this reference number. The customs broker manually enters the same reference number into the e2m when lodging for customs declaration. Upon the inspection of the shipment, the BOC inspector determines the status of each PNSW application based on the reference number entered into the e2m. The BOC inspector then verifies the status of each application by searching through the PNSW system.

14. Note that the customs brokers submit the transaction reference numbers through the e2m to enable the BOC customs officer to view and verify the traders’ approved permits and clearances in the PNSW site. Once the traders’ permits or clearances are inspected, the customs officer fills up a Customs Inspection Record that, if saved in the PNSW system, automatically tags the permits as used. This enables the participating government agencies issuing the permits to receive immediate feedback through the PNSW system and determines which of the permits issued by the said agencies have been tagged by the BOC as having been utilized in relation to a release order, and is disabled for further use by any

---

56 Information found in the FAQs of the PNSW Website.
57 Under Section 27 of Republic Act 9280, otherwise known as the Customs Brokers Act of 2004, only customs brokers can apply for and sign import and export entry declarations.
58 Proposed Draft of Customs Memorandum Order (currently unnumbered), “Guidelines in the Verification of Import/Export Permits/Clearances and their Tagging as Used through the PNSW”. 

- 14 -
Nevertheless, to facilitate cargo release, the BOC is still required to separately process the customs brokers’ import entry through its e2m system.

15. In the event that the goods examined or the details in the Single Administrative Document (SAD) declaration do not conform with the details in the permits issued by the participating government agencies found in the PNSW site, the customs officer shall click a “transfer workflow” button in the site which transfers the information back to the participating government agency concerned, and informs the trader of the rejection of the permit issued for reasons indicated by the customs officer in the “remarks” box that can be viewed in the site as well. The BOC suspends the processing of the import entry and the release of the cargo in the meantime, until an acceptable permit has been re-submitted.

16. The Crown Agents’ Systems Maintenance Contract with BOC has expired on October 21, 2012. The BOC will open for public bidding, the engagement for a service provider for Phase 2 of the PNSW Project.

17. It is expected that in Phase 2 of the implementation of the PNSW, more participating government agencies, including the BOC’s e2m, will be finally linked with the PNSW. Also, it is expected that the online payment will be fully operational, data requirements and the forms of the participating government agencies will be simplified, harmonized, and standardized, and the system will be finally integrated with the ASW.

CONCLUSION

- The PNSW does not, as of yet, conform to the requirement of a single point of entry for the submission of data and information that is characteristic of a NSW.
- Many of the participating government agencies are not yet linked to the PNSW, and most are only partially linked and still rely on their own respective systems.
- We note that the BOC currently facilitates the processing of import and export declarations and clearances outside of the PNSW through e2m, where traders/brokers access the services of several VASPs online where they register and lodge their permit or clearance applications.

---

59 Ibid.
60 Ibid.
61 Ibid.
62 As confirmed by Ms. Sally S. Alvareda of Crown Agents (Agency Coordination and TWG Meeting No. 6, Bureau of Customs, August 2, 2012).
63 Ibid.
The same is true for PEZA. PEZA's Electronic Import Permit System (eIPS), processes and generates electronic Import Permits (eIP) filed by PEZA-registered traders/brokers that are routed to the websites of three (3) accredited VASPs. The said permits are conveniently paid online through an e-payment gateway developed by the VASPs with their partner banks. All eIPS-approved IPs are then electronically transmitted to PNSW by the VASPs.

The DA also has its own DA Trade System where applications for permits or import clearances are lodged and processed. Only the approved permit and clearances are transferred to PNSW via system interface for tagging by the BOC.

The Bureau of Internal Revenue's processing of its Authority to Release Imported Goods (ATRIG), which clearance is required by the BOC to release excisable imported articles, is still done outside of the PNSW.

The processing of the clearances by the Dangerous Drugs Board (DDB) for products not included in the list of dangerous drugs, and the issuance of certificates of exemption to companies importing controlled chemicals or substances, is not yet part of the PNSW.
A. Enabling the Single Window

Establishment of the NSW in National Law

1. Under the Philippine Constitution, the Philippine legal system recognizes the legislative branch as the source of national law. Statutes must be passed by a majority vote in both chambers of a bi-cameral legislature, and approved by the President. The executive branch may issue “delegated legislation” i.e., administrative regulations, which may come in the form of executive orders, department orders, or administrative circulars, etc. Regardless of its designation, under the separation of powers doctrine, such regulations:
   a. Can only interpret or implement a given statute;
   b. Must be based on a valid delegation of authority;
   c. Must be in harmony with the provisions of law; and
   d. Cannot add to or diminish substantive legislation.

2. The Philippine Legal System makes a distinction between substantive law and procedural law. Substantive laws are enacted by the legislature and deal with the creation, definition or regulation of rights, or the power of government agencies or instrumentalities. Procedural laws are enacted by the Supreme Court and prescribe rules and forms of procedure for the enforcement of rights in the courts.

3. Philippine jurisdiction recognizes the binding authority of international legal instruments. Treaties entered into by the country occupy the same status as that of a local law once ratified by two-thirds (2/3) of Philippine Senate.

4. Not all international instruments executed by representatives of the Philippine Government require ratification to have legal effect. The Philippine legal system distinguishes between treaties and mere executive agreements. International agreements that involve policy or create arrangements of a permanent character

---

64 Executive issuances from the time President Ferdinand Marcos had legislative powers under his martial law authority, and briefly, under President Corazon Aquino after the 1986 Revolution, have the status of legislative enactments. To the extent that laws passed by the legislature have not superseded these executive issuances, they remain effective.

65 Despite the subsidiary nature of administrative regulations, they are nevertheless imbued with the "force and effect of law", which means that they are presumed to be valid and have full and binding effect [US v. Tupasi Molina, 29 Phil. 119 (1914)]. Furthermore, administrative regulations are “entitled to the greatest weight by the Court construing such rule or regulation, and such interpretation will be followed unless it appears to be clearly unreasonable or arbitrary [Geukeko v. Araneta, 102 Phil. 706 (1957)]. The Philippine Legal System further makes a distinction between the substantive law promulgated by the legislature, which may create rights or allocate the powers among government agencies, and remedial law, issued by the Supreme Court and regulates practice and procedure before the courts [Pineda v. de Guzman, 21 SCRA 1450 (1967)].

are regarded as treaties and therefore require the concurrence of the Senate.\footnote{Commissioner of Customs vs. Eastern Sea Trading, G.R. No. L-14279 (1961).} On the other hand, those agreements between the Philippines and other countries that merely embody adjustments of details to the implementation of established policies or those that involve temporary arrangements are considered mere executive agreements and do not require ratification from the Senate.\footnote{Ibid.}

5. To the extent that the ASW Agreement and the ASW Protocol provide directions for the implementation of NSWs, they shall be treated in this gap analysis as part of the PNSW’s legal framework.

6. The Philippine Legislature has passed no substantive law mandating the establishment of an NSW. Neither is there pending legislation to this effect.

7. The current implementation of the PNSW traces its legal mandate to EO 482,\footnote{Executive Order 482 - Creating the National Single Window Task Force for Cargo Clearance, EO, 2005.} issued by the Office of the President on December 27, 2005. Briefly, EO 482 provides for the formation of a Task Force charged to create the PNSW and to oversee its integration with the ASW.

8. The PNSW Task Force is comprised of a Steering Committee for high-level functions. The Steering Committee is chaired by the Secretary of the DOF and composed of the following members:
   a. Secretary of the DTI;
   b. Secretary of the DA;
   c. Secretary of the DOTC;
   d. Secretary of the DILG;
   e. Secretary of the DOH;
   f. Governor of the BSP; and
   g. Director-General of the NEDA.

9. Under EO 482, the PNSW-SC was empowered to “set policy guidelines for the creation and operation of the NSW and the ASW”.\footnote{Ibid., sec. 3.} The PNSW-SC is essentially the central management authority of the PNSW project tasked to ensure the effective and efficient implementation of the PNSW and ASW.\footnote{Ibid., sec. 4(c).}

10. EO 482 also established the PNSW-TWG presided by the Commissioner of Customs and composed of designated representatives from the following participating government agencies:
   a. CICT;
   b. BIR
   c. TC;
   d. PPA;

\footnote{Ibid.}
11. The PNSW-TWG reports directly to the PNSW-SC and is tasked to perform the following:

a. Implement the policies and directives of the PNSW-SC;
b. Identify definitions and data sets required for integration;
c. Delineate the roles and responsibilities of each participating government agency;
d. Create the conceptual framework and other similar instruments required for integration.
e. Comply with all other instructions from the PNSW-SC.73

12. On February 10, 2012, nearly all the participating government agencies involved with the PNSW, save for the BIR, signed the PNSW MOA. The agreement provides some guidance in areas of the NSW that were not covered by EO 482 such as:

a. Use of data formats that are functionally equivalent to their paper counterparts;74
b. Confidentiality and security of data;75
c. Information sharing;76 and
d. Registration and authentication of private sector users.77

13. EO 482 and subsequent administrative issuances ultimately trace their authority from the legislative charters creating the agencies in the PNSW Task Force, as well as the Executive branch’s power to control, and supervise its agencies.

14. Using administrative regulation and a contractual/MOA model as the primary legal framework for implementing the PNSW enables the government to proceed expediently and avoid delays that usually accompany a protracted legislative process. In contrast, administrative regulations are issued without protracted negotiations and may be enacted immediately.

---

72 Ibid., sec. 5.
73 Ibid.
75 Ibid., sec. 4.
76 Ibid.
77 Ibid., sec. 5.
Government Electronic Payment and Collection System

15. Enabling electronic payment is an important part of the PNSW system. Payment is required for approving applications of traders for mandatory permits and issuances. Only paid applications are approved by the participating government agencies and uploaded into the PNSW system, which are then viewed and verified by a customs officer of the BOC before it releases cargo.

16. Agencies are mandated to adopt an Electronic Payment and Collection System (EPCS) under Philippine Law. The legal framework for the EPCS is Republic Act 8792, or the E-Commerce Act (ECA) and two Joint Department Orders issued by the DOF and DTI.78

17. The ECA directs government agencies to adopt an online payment system by mandating that government agencies should require and accept payments and acknowledge such payments by issuing receipts, through systems using electronic data messages or electronic documents.79

18. In adopting an online payment system, agencies must also observe the principles of technology neutrality, interoperability, and auditability as provided by the Act’s Implementing Rules.80

19. In order to fully implement this mandate, DOF and DTI issued the Guidelines Implementing RA 8792 on EPCS in Government (“Guidelines”).81 The Guidelines require agencies to accommodate various modes and channels of electronic payments (with due regard to the principles of technology neutrality, interoperability, and auditability). It also requires that agencies adopt systems to:

   a. Serve as primary interface between the agency and the client;
   b. Maintain records and generate payment and collection reports (stored in Active File for 60 days, and, later, in Electronic Archives for 10 years);
   c. Secure confidentiality, privacy, integrity, and availability of electronic information; and
   d. Provide technical support and customer help desk.82

20. The Government Electronic Payment and Collection System Evaluation Team (GEPSCE), which was created to evaluate and approve applications in the adoption of EPCS, is tasked to:

   a. Keep a list of accredited Electronic Payment Gateway Providers (EPGP);
   and
   b. Conduct a post-system audit of an approved EPCS.83

---

78 DTI-DOF Joint Department Administrative Order No. 2, issued on 26 October 2006, and DTI-DOF Joint Department Administrative Order No.10-01, issued on 24 March 2010.
81 DTI-DOF JDAO No. 2, Series of 2006 (October 25, 2006).
82 Ibid., sec. VII.
21. DTI-DOF Joint Department Administrative Order No. 10-01, Series of 2012 on the use of Access Devices for payment of government fees through the EPCS allowed the government agencies to:

   a. Use “Access Devices” (credit cards, debit cards, cash cards, and mobile phones) for payment; and
   b. Collect, in behalf of the EPGP, “Convenience Fees” (paid for the convenience of having an alternative mode of payment, i.e. through Access Devices).84

Note, however, that even before the issuance of this JDAO, Philippine Law has long recognized the use of such access devices in commercial transactions (Access Devices Regulation Act of 1998).85

22. An EPGP is only allowed to partner with either an Authorized Government Depository Bank (AGDB) or an Authorized Agent Bank (AAB) in processing online payments because of the general prohibition among government agencies to maintain deposits in private banking institutions.86 As an exception, a private bank can be designated as an AGDB if authorized by the DOF and the Monetary Board.87 However, to be part of the EPCS of government agencies, the AGDB or AAB must have an existing Internet Banking facility approved by the BSP.88 Also, Service Agreements with EPGPs must be consistent with the E-Commerce Act (Sec. 16-26 and 30-32) and must contain dispute resolution mechanisms.89

Gaps and Recommendations

- Although EO 482 provides a readily available framework for coordination among the participating government agencies, it does not provide details that are critical for the effective and efficient implementation of the PNSW or its long-term viability.

- In its current incarnation, the PNSW Task Force does not have a legal personality separate from that of its members. Neither does it have a legally defined set of mandates or powers. This presents a complication whenever the PNSW Task Force needs to enter into transactions. It cannot by itself enter into contracts necessary to implement or maintain the PNSW. Legal representation for such

83 Ibid., sec. VIII.
84 DTI-DAO JDAO No. 10-01, Series of 2012 (March 24, 2010), sec. IV.
85 Republic Act No. 8484 (February 11, 1998).
86 DTI-DOF JDAO No. 2, Series of 2006, Section VII (B) (October 25, 2006).
87 Ibid, sec. VI.
88 Ibid.
89 DTI-DAO JDAO No. 10-01, Series of 2012 (March 24, 2010), sec. VII, B(1).
contracts may have to be performed jointly by all the participating government agencies, or based on current practice, by the BOC.

- Although EO 482 provides for the basic organizational structure and leadership of the PNSW Task Force, it does not provide for formal decision-making processes and consequent lines of accountability. Based on EO 482, both policy-setting powers and implementation details are handled by collective bodies, requiring a majority for each decision. No delegation of executive authority to carry out time- and mission-critical components of the project is specified in either EO 482 or the PNSW-SC’s policy issuances.

- Philippine laws that establish a standing organization with its own legal personality and mandate usually include provisions for funding, implemented through the earmarking of a specific source of funds (i.e. NSW processing fees, or a specific portion of customs duties). Other than a general instruction to the Steering Committee to come up with “financial schemes or strategies”, neither EO 482 nor the policy issuances of the PNSW-SC, outline a clear long-term plan for the PNSW’s funding and financial viability.

- Currently, the PNSW is funded through a specific item in the BOC’s annual budget. Without a specific source of funds earmarked for the implementation and maintenance of the PNSW, the necessary amount would have to be renegotiated annually in the government’s budget, as reflected in the GAA.

- The Philippines should pass national legislation for the implementation and maintenance of the PNSW. Such a law should include provisions for:
  - Creation of new government entity tasked as a specific implementing and administering authority for the PNSW with an organic relationship with the project’s core stakeholders (i.e. the BOC or the DOF.);
  - Delineation of functions and coordination between the notional implementing/administering authority and other participating government agencies.
  - Delegating executive powers for time- and mission-critical project components to a single executive officer; and
  - Specific budgetary allocation, with stipulation as to source of funding, i.e., from fees that the PNSW is authorized to collect.

- Although such proposed legislation should point to the mandate and powers of the notional PNSW administering authority, the law should
nevertheless give this agency sufficient leeway to choose how it can implement the NSW project, such as:

- Developing and maintaining subsequent modules of the NSW system in-house;
- Outsourcing development and maintenance of subsequent modules of the NSW, employing from a spectrum of partnership configurations with the private sector (i.e. Build-Operate-Transfer or Build-Lease-Transfer schemes); and
- Allowing and encouraging participating government agencies, to the fullest extent possible, to develop, operate and maintain their own independent systems to which the PNSW system can interconnect.

- National legislation will reflect the strong political will and support to the PNSW. Such a show of commitment can bolster the viability of the PNSW, and signal to the participating government agencies that they are expected to prioritize the requirements of the PNSW over their internal projects that may conflict with, or be redundant to, the PNSW.

- In the interim, the Office of the President may consider amending EO 482 to provide incremental improvements to the current legal framework to provide for a more coherent delineation of work and coordination among agencies, mechanisms for monitoring, oversight, and accountability and sustainability.

- Coordinate with the Supreme Court for the development of specialized courts, rules, or training for judges that can facilitate adjudication of PNSW-related controversies. Such courts (or administrative adjudicative bodies) should be intimately familiar with the PNSW’s electronic workflow, customs law, as well as the ECA and electronic evidence provisions relevant to PNSW transactions.

- In relation to the implementation of a government electronic payment system, Section 69 of Presidential Decree No. 14445 (Government Auditing Code) provides that only “public officers” are authorized to receive and collect moneys arising from payment of government assessments.

- It is recommended that the present law be amended to allow government agencies to appoint another government agency or engage private agencies to collect fees and issue official receipts in their behalf.

- We also note Section 68 of the Government Auditing Code that provides that “no payment of any nature shall be received by a
<table>
<thead>
<tr>
<th>Gaps and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>collecting officer without <em>immediately</em> issuing an official receipt in acknowledgment thereof.&quot; Similarly, Section VII of the Guidelines also provides that the EPCS of the government agency should be able to generate and issue electronic proof of payment or electronic receipts.</td>
</tr>
</tbody>
</table>

- The present practice by the participating government agencies of uploading mere electronic voucher receipts may not be sufficient, as it is not clear whether electronic voucher receipts are legal equivalents of official receipts under Philippine law. For audit purposes however, the Commission on Audit (COA) issued the Guidelines and Principles on the Acceptability of the Evidence of Receipt of Payment for Disbursements (COA Guidelines), 90 that recognized that while the pre-printed official receipt is the traditional artifact recognized by government auditors as evidence of receipt of payment, this traditional mode is not applicable in cases of electronic transactions like credit card payments and e-payments.91 Note that the BIR has not issued similar guidelines for taxation purposes.

- A law should be passed recognizing and authorizing issuance of electronic official receipts and providing therefor the requirements for such issuance.

---

**E-Commerce and Electronic Transactions under National Laws**

23. The ECA gives legal recognition to electronic data messages and electronic documents. Patterned after the UNCITRAL Model Law and Singapore’s ETA, the ECA is guided primarily by the “functional equivalence” approach. Under this approach, if the functions of a document are considered, and if an equivalent exists in electronic form, then the latter will be adopted.92

24. This approach is reflected in the PNSW MOA that provides that parties to the agreement “shall use data in electronic format that is functionally equivalent to paper-based documents.”93

---

91 Ibid., sec. 1.
92 For example, a signature’s function is to identify the signer and indicate his consent to a document. If an electronic method performs the same functions, then such method would be considered an electronic signature.
93 *Memorandum of Agreement on the Implementation of the Philippine National Single Window*, sec. 3.
25. Pertinent to customs operations and the PNSW, the ECA applies the same recognition to commerce in the carriage of goods. In particular, the ECA provides that should the law require any action on the carriage of goods (i.e. claiming delivery, authorizing release) to be in writing or a paper document, such requirement is met by the use of electronic data messages or electronic documents. The same applies when the law imposes consequences for failure to carry out the action or use a paper document.  

26. The ECA is supplemented by its Implementing Rules and Regulations (ECA-IRR) that provide implementation details and reflect the contemporaneous interpretation of the concerned administrative agencies.

27. The ECA adopts the principle of non-discrimination, stating that electronic documents “shall have legal effect, validity or enforceability as any other document or legal writing.”

28. Under the ECA’s recognition regime, should any legal requirement specify that a document be in writing, such requirement is met by an electronic document that “maintains its integrity, reliability and can be authenticated so as to be usable for subsequent reference.”

29. Even prior to the passage of the ECA, there was no dispute as to the validity of electronic contracts and transactions since the Philippine contract law adheres to the “spiritual system” of contracts. Hence, the ECA expressly validates electronic contracts without displacing the substantive Philippine laws on contracts. The ECA merely articulates the view that elements of offer and acceptance or its external manifestations, may be expressed in electronic forms.

30. However, despite many textual similarities with the UNCITRAL Model Law, the ECA’s approach to electronic documents diverges significantly with the Model Law, particularly the latter’s distinction between a “writing” and an “original”.

31. Under the Model Law, an electronic data message that qualifies as an electronic “writing” will suffice to meet the legal requirement of being embodied in a “written document” or be “in writing”. An electronic data message will be deemed “written” as long as it is “accessible so as to be usable for subsequent

---

94 ECA, secs 26–27.
96 Ibid., sec. 7(a). The same section of the ECA offers as standards for meeting this condition the following: (1)The electronic document has remained complete and unaltered, apart from the addition of any endorsement and any authorized change, or any change which arises in the normal course of communication, storage and display; and (2)The electronic document is reliable in the light of the purpose for which it was generated and in the light of all the relevant circumstances.
97 Article 1356 of the Civil Code provides that “(c)ontracts shall be obligatory, in whatever form they may have been entered into, provided all the essential requisites for their validity are present”.
reference”.99 “Writings” are not required to meet standards of integrity, inalterability or reliability.

32. On the other hand, the Model Law distinguishes an “original” from “writings”. The Model Law requires “originals” to have “a reliable assurance as to the integrity of information” it contains, in addition to the capacity “being displayed to the person to whom it is to be presented “in cases where the law requires presentation.100

33. The ECA does not adapt this clear distinction between “writings” and “originals”. Instead, the ECA applies the requirements of integrity and reliability not only to “originals” but to “writings” as well. 101

34. Integrity for “writings” is established by showing “(i)t has remained complete and unaltered, apart from the addition of any endorsement and any unauthorized change, or any change which arises in the normal course of communication, storage and display.”102 Reliability, on the other hand, would be weighed based on the “purpose for which it was generated and in the light of all the relevant circumstances.”103

35. Integrity for “originals”, on the other hand, must be shown to exist “from the time when it was generated in its final form”.104

36. The application of reliability standards to both classes of documents is not only incompatible with the Model Law but may be unduly restrictive, especially when applied to a cross-border setting. Removing these requirements will not strip “writings” of all legal effect. Taking into consideration the functional equivalence principle, “writings” under the ECA may still be admitted for purposes that do not require originals and may be given probative weight by the court.

37. The scope of what may legally be recognized as an electronic document is further restricted by decisions of the SC. In MCC Industrial Sales v. Ssangyong, the SC adopted the view that the original print-out from a fax machine (or its subsequent photocopies) are not electronic data messages or electronic documents.105

38. The court reasoned that in ordinary fax messages, i.e. those that do not originate from a general purpose computer, the fact that the fax print out can be traced to a paper original puts it beyond the legislative contemplation of electronic documents.106 This further shrinks the subset of electronic documents that will enjoy recognition under the ECA to those that originate from electronic systems.

---

99 Ibid.
100 For example, the original of a negotiable bill of exchange must be presented to the drawee for acceptance.
101 Republic Act 8792 - Electronic Commerce Act, sec. 7(a) vis–a–vis 7(c).
102 Ibid., sec. 7(a)(i).
103 Ibid., sec. 7(a)(ii).
104 Ibid., sec. 7(c)(i).
105 MCC Industrial Sales Corporation V. Ssangyong Corporation (2007).
106 See also Ellery March Torres V. Philippine Amusement and Gaming Corporation (2011).
39. Rather than put electronic documents in parity with regular documents, the decisions establishes a rift with paper-based documents (including faxes) requiring compliance with the authentication rules under ROC on one side, and electronic documents to be authenticated under the REE as enacted by the SC upon the other. The decisions further leave doubt whether electronically scanned documents which originated as paper documents (which go through the same process as a fax) fall under either or both categories. In this sense, it appears that Philippine law is more stable with respect to electronic documents that originate electronically rather than those with paper-based origins.107

40. In the context of the PNSW, it appears therefore that to forestall the possibility that the documents processed therein are considered to be paper documents by the courts, the PNSW system must be designed to ensure that all electronic documents it utilizes or issues originate electronically. This will ensure the applicability of the REE and facilitate their admission into evidence.

41. However, the bifurcated treatment of paper and electronic documents can be solved if the Supreme Court were to incorporate the REE into the rules on evidence embodied in the ROC. In this way, both electronic and paper documents would be treated the same way and will fall under the rubric of documentary evidence.

Notarized Documents

42. The current PNSW workflow often requires the submission of notarized documents for some regulatory requirements. Notarization means the certification by a notary public to establish the authenticity of a signature and the voluntariness of the consent or authentication of a relevant document. The personal appearance of the person who executed the document before a notary is mandatory.

43. The Philippine legal system requires a notary public’s acknowledgement for some documents to be valid.108 Although notarization is often not required for authenticity or legal enforceability of documents, notarized documents are often preferred because the ROC deem them to be public documents, and are thus easier to present in evidence.109 The public document status provides certain advantages from an evidentiary standpoint as it gives documents the presumption of authenticity.

44. The notarization of documents still occupies a leg of the workflow that is offline. In the current iteration of the PNSW, documents that require notarization would have to be downloaded from the PNSW website or the website of the regulatory agency.

107 It would appear, based on the text of the *Ssangyong* decision, that a fax message which was originally composed and sent through a general purpose computer would qualify as an electronic document.

108 For example, a formal will is required to be notarized, and signed by three witnesses; otherwise, such will is invalid and the decedent is deemed to have died intestate.

concerned. There are no rules that enable or implement electronic notaries or electronic notarization.

45. The PNSW as well as the participating government agencies should re-examine the notarization requirement for most of the documents in the PNSW workflow. With the proper mix of technologies and practices, alternative authentication mechanisms (i.e. electronic signatures supplemented with certification authorities and security policies) can match, if not exceed, the value assigned to notarized documents in terms of authenticity and reliability.

46. Should the PNSW or the participating government agencies insist on notarization requirements, it would be advisable to coordinate with the SC to develop and implement rules for electronic notarization.

Electronic Transactions with Government

47. The ECA further enables transactions with government agencies, providing that within two (2) years from passage of the law, government offices should transact business electronically. However, more than a decade from the passage of the ECA, this goal has not been met. Note that the counterpart provision of the ECA-IRR clarifies that law cannot be used by private citizens to require government agencies to transact electronically. 110

48. Implementation of the ECA’s mandate for computerized government transactions has been slow and uneven. Most of the participating government agencies do not have end-to-end systems for accepting and processing electronic documents submitted for their regulatory requirements. Thus, these agencies have not had the opportunity to operationalize the ECA’s treatment of electronic documents for their internal processes.

49. Other agencies, on the other hand, have implemented their own electronic permits processing system and their own internalization of the ECA provisions on the acceptability of electronic documents.

50. These systems vary in terms of sophistication, scope, and the degree to which they overlap with PNSW functionality. For example, PEZA, the authority overseeing Philippine free trade areas, has built its own EIPS for accepting and processing import permit applications. This system has a significant function overlap with the PNSW system, to the extent that the PEZA has largely eschewed use of the current PNSW implementation in favor of its EIPS for its entire import permit processing requirements. 111 All EIPS-approved permits are electronically transmitted to VASPs, and the PEZA does not see the need to port its import permit workflow into the PNSW.

---

111 The BPI has its own Sanitary and Phytosanitary Import Clearance System as mandated by Department of Agriculture Administrative Order No. 08-10, 2010.
51. In the case of the taxing authority, the BIR has a suite of systems (along with complementary rules) for the submission of tax information by electronic means. The BIR’s EFPS is adopted by taxpayers on a voluntary basis. The EFPS adopts the ECA’s treatment of electronic documents.\(^{112}\) The BIR likewise allows the submission of electronic documents in the context of tax audits and investigations. Nevertheless, the BIR’s implementation is still not an end-to-end solution. For some transactions, they involve submission of taxpayer information encoded into files (usually through electronic versions of tax forms) and transmitted via storage media or email. They exist as discrete systems that are not currently integrated with the PNSW.

52. Some documents in the PNSW workflow also require the presence of a documentary stamp issued by the BIR upon the payment of a DST. Under the current implementation of the PNSW, the DST is paid offline, evidenced by a printed stamp that is then physically attached to a document. The BIR has a separate electronic system for receiving payments for and issuing documentary stamps. The current implementation of the PNSW does not communicate with this system.

### Gaps and Recommendations

<table>
<thead>
<tr>
<th>Gaps and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>- For greater stability and a more standard understanding of the law on electronic documents, the ECA should be amended to conform to the language of the UNCITRAL Model Law on Electronic Commerce, as well as to the ECC).(^{113}) The ECC, which builds upon, the Model Law, reiterates the principles of functional equivalence, technological neutrality, and non-discrimination. At the same time, the ECC updates the Model Law to take into account the cross-border nature of some electronic transactions.</td>
</tr>
<tr>
<td>- To avoid the separate treatment of paper and electronic documents for evidentiary purposes, the SC can integrate the REE into the rules on evidence. This will establish both as documentary evidence requiring consistent and uniform treatment thereof for evidentiary purposes. This also furthers the functional equivalence doctrine embodied in the ECA.</td>
</tr>
<tr>
<td>- The PNSW participating government agencies should re-examine their workflow to evaluate the legal necessity for notarization given the absence of any rules governing electronic notarization. If a document in a particular workflow is legally required to be notarized, then it should be treated as a paper document subject to the provisions of the ROC on evidence. The REE will not be applicable.</td>
</tr>
</tbody>
</table>

\(^{112}\) Revenue Regulation 09-01 - Electronic Filing of Tax Returns and Payment of Taxes, RR, 2006.

Gaps and Recommendations

- Moving forward, the PNSW Task Force should consider coordinating efforts with the SC with respect to the rules on electronic notarization.

- Based on the significant (yet uneven) pace of the various efforts to computerize government transactions are proceeding, the PNSW Task Force or any future PNSW administering authority can consider implementing the PNSW not as a monolithic system but as middleware tier, brokering between the various systems already implemented. To achieve true end-to-end integration with the PNSW, the participating government agencies should closely monitor their technology choices and structure procurement with a view to future integration. Stakeholders should be mindful that technology choices have legal implications that may extend beyond the original milieu where the technology is applied. At the same time, the existing legal framework can enable or constraint technology choices down the road.

Acceptance of Electronic Records in Judicial and Administrative Processes

53. The acceptance of the validity of electronic documents as enshrined in the ECA would be hollow without complementary provisions in procedural law that enable the presentation and admission of electronic documents in judicial or administrative proceedings.

54. Although the ECA itself enables or facilitates the presentation of electronic documents in formal evidentiary proceedings, this treatment was implemented in a parallel set of rules under the REE. These rules were originally applicable to “civil actions and proceedings, as well as quasi-judicial and administrative cases,” but were later revised to include criminal cases.114

55. For evidentiary purposes, the ECA expressly provides that electronic documents are the functional equivalent of paper documents.115 This is correlated with the non-discrimination of data messages and electronic documents as provided for under Section 6 and 7 of the ECA.116 These should be read in conjunction with Section 10 of the ECA-IRR that expands the requirements an electronic document should meet to be considered a “writing” under Philippine law. Note that where

114 See Supreme Court Resolution, No. 01-7-01-SC (2002).
115 See footnote 95 supra.
116 Section 6. Legal Recognition of Data Message. - Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the data message purporting to give rise to such legal effect, or that it is merely referred to in that electronic data message.
117 See footnote 95 supra.
national laws require that information be “in writing” or be embodied in a “written document” (i.e., the Statute of Frauds),\textsuperscript{118} such requirement is met by an electronic document or electronic data message. As discussed above, “writings” are further subject to integrity and reliability requirements.

56. Operationalizing the non-discrimination principle, the ECA states that electronic documents shall not be denied admissibility on the \textit{sole} ground that it is in electronic form or it is not the standard form.\textsuperscript{119} This does not, however translate to the automatic admissibility of electronic documents. Electronic documents, just like any documents submitted in evidence, should meet the standards specified in the ROC, specifically in the REE.\textsuperscript{120}

57. The REE integrates the ECA’s adoption of the functional equivalence principle, as well as its non-discrimination against electronic documents in determining admissibility in evidentiary proceedings.

58. The REE implements Section 7 of the ECA which provides that “(f)or evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws.” Consequently, electronic documents and electronic data messages are documentary evidence under the ROC. The ROC requires that documentary evidence be subject to a process of authentication prior to admission as evidence. The REE provides for methods of authentication specific for electronic documents.

59. The Philippine legal system adopts the “best evidence” rule, which requires that the “originals” of the documents be presented for certain assertions of facts. The ECA expressly modifies this rule by stating that legal requirements for the originals are “met by an electronic data message or electronic document”, as follows:

\begin{enumerate}
\item The integrity of the information from the time when it was first generated in its final form as an electronic data message or electronic document is shown; and
\item That the information is capable of being displayed to the person to whom it is to be presented.\textsuperscript{121}
\end{enumerate}

\textsuperscript{118} Under Article 1403(2) of the Philippine Civil Code, the following agreements should be embodied in writing:
\begin{enumerate}
\item An agreement where the terms are to be complied with a year after the agreement;
\item A special promise to answer for the debt, default, or miscarriage of another;
\item An agreement made in consideration of marriage, other than a mutual promise to marry;
\item An agreement for the sale of goods worth more than PHP 500;
\item A lease agreement for real property, if the lease is longer than one year;
\item A sale of real property;
\item A representation to the credit of a third person.
\end{enumerate}

\textsuperscript{119} Republic Act 8792 - Electronic Commerce Act, sec. 17.

\textsuperscript{120} Specifically, that the evidence be relevant, and not otherwise disqualified by a specific provision of the RROE. See Rule 128, Section 3, ROC. Relevance requires “…a relation to the fact in issue as to induce belief in existence or non-existence…”, ibid., Section 2.

\textsuperscript{121} Republic Act 8792 - Electronic Commerce Act, sec. 10.
60. The same provisions of the ECA provide that the integrity of the electronic document shall be assessed based on:

   a. Whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and
   b. The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all relevant circumstances.\textsuperscript{122}

61. The REE effectively amends the ROC in providing that “(a)n electronic document shall be regarded as the equivalent of an original document” if:

   a. It is a printout or output readable by sight or other means;
   b. It is shown to reflect the data accurately.

62. Section 2 of the same Rule enables the presentation of duplicate originals or copies “executed at or about the same time with identical contents” or counterparts. These duplicates shall be considered as equivalent of an original.\textsuperscript{123}

63. In \textit{MCC Industrial Sales v. Ssangyong}, the SC adopted the view that the original print-out from a fax machine or its subsequent photocopies are not electronic data messages or electronic documents\textsuperscript{124}, and therefore refused to apply the said rule on duplicate originals. Instead, the SC ruled that the original documents – not the fax copies, should be presented in evidence.

64. Given the variance in the best evidence rule in the ROC and the REE, the status of the document as either electronic or paper-based, determines the form of the evidence admissible in court. As stated earlier, duplicate originals (such as print-outs or photo copies) would suffice for electronic documents but not for paper documents.

65. The separate treatment of paper and electronic documents however can be addressed by the integration of the REE into the ROC. In this way, paper and electronic documents will fall under a single category: documentary evidence.

66. Rule 5 of the REE mirrors the text of the ECA in establishing that the party who seeks to introduce an electronic document in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting the relevant point of fact, i.e., that the electronic document is what the party making the assertion claims it to be. Failure to authenticate under the Rule 5 of the REE means that an electronic document cannot be admitted into evidence.\textsuperscript{125}

\textsuperscript{122} Ibid.
\textsuperscript{124} MCC Industrial Sales Corporation V. Ssangyong Corporation, G.R. No. 170633, October 17, 2007.
\textsuperscript{125} Ibid. Rule 5, sec. 1.
67. The REE provides three modes through which an electronic document may be authenticated. According to Rule 5, authenticity may be established by presenting:

   a. Evidence that the electronic document has been digitally signed;
   b. Evidence that other appropriate security procedures or devices as may be authorized by the Supreme Court or by law for authentication of electronic documents were applied to the document; and
   c. Evidence showing its integrity and reliability to the satisfaction of the judge.126

68. *Aznar v. Citibank*, which involved a print out purported to originate from a computer system, interprets the authentication requirement for electronic documents to involve a duty of the proponent to “demonstrate how the information reflected in the print-out was generated and how the said information could be relied upon as true.”127

69. Separate from the issue of admissibility after the electronic evidence has been duly authenticated is the issue of evaluating the probative weight of electronic documents admitted into evidence. The REE puts forward the following factors for consideration of the court:

   a. The reliability of the manner or method in which it was generated, stored or communicated, including but not limited to input and output procedures, controls, tests and checks for accuracy and reliability of the electronic data message or document, in the light of all the circumstances as well as any relevant agreement;
   b. The reliability of the manner in which its originator was identified;
   c. The integrity of the information and communication system in which it is recorded or stored, including but not limited to the hardware and computer programs or software used as well as programming errors;
   d. The familiarity of the witness or the person who made the entry with the communication and information system;
   e. The nature and quality of the information which went into the communication and information system upon which the electronic data message or electronic document was based; or
   f. Other factors which the court may consider as affecting the accuracy or integrity of the electronic document or electronic data message.128

70. For evaluating the integrity of an information and communication system at this stage, the REE likewise provides the following factors for consideration:

   a. Whether the information and communication system or other similar device was operated in a manner that did not affect the integrity of the electronic document, and there are no other reasonable grounds to doubt the integrity of the information and communication system;

---

126 Ibid. Rule 5, sec. 2.
128 Ibid., Rule 7, sec. 1.
b. Whether the electronic document was recorded or stored by a party to the proceedings with interest adverse to that of the party using it; or
c. Whether the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not act under the control of the party using it.129

71. The REE further provides for the admissibility of audio, photographic and video evidence. It also enables the presentation of ephemeral electronic communications.

72. The REE also provides for the admissibility of electronic business records130 and permits entry into evidence in judicial proceedings upon the testimony of the custodian or other qualified witnesses. This represents a departure from the ROC governing paper-based records which may be admitted if they are authenticated by the person who has actual knowledge of the facts stated therein – only upon the latter’s death or unavailability will the courts allow the records to be admitted as proof of their contents131. Hence, the REE establishes a bias in favor of electronic records in the sense that they are more easily presented into evidence in court.

Gaps and Recommendations

- The PNSW should study which of its documents are paper-based and which are electronic and provide for guidelines for their admissibility into evidence in the event of litigation.

- In the long run, the PNSW Task Force should consider encouraging the SC to treat both electronic and paper documents as documentary evidence under a single set of rules in the ROC. This will entail incorporating the REE into the ROC’s rules on evidence.

B. Data Protection and Information Security

73. Recommendation 35 contains no explicit definition or standards for “data protection” and “information security”, albeit it correlates these terms to the following concepts:

a. Security and access protocols established through identification, authentication, and authorization mechanisms;

---

129 Ibid., Rule 7, sec. 2.
130 Ibid., Rule 8, secs. 1 & 2.
131 ROC, Rule 130, sec. 43.
b. Risk analysis in finding vulnerabilities with a view to avoiding data breaches; and,
c. Privacy and confidentiality.\textsuperscript{132}

74. The ASW Agreement does not contain an explicit commitment to these concepts. The Agreement’s enumeration of implementation principles\textsuperscript{133} contains no reference to security or privacy. Nevertheless, the provision that urges member states to “make use of information and communication technology that are in line with relevant internationally accepted standards”\textsuperscript{134} for NSW implementations can be construed broadly enough to incorporate a general responsibility to maintain standardized data protection and security arrangements.

75. The subsequent ASW Protocol, on the other hand, provides that NSWs and the ASW should feature a “secure infrastructure” that shall “...follow international standards and best practices with features such as confidentiality, data integrity, authenticity, and non-repudiation.”\textsuperscript{135}

76. Whenever applicable, the gap analysis will refer to well-accepted international standards in evaluating the extent to which the existing legal framework addresses data protection, information security and privacy, and related concepts.

77. Details on the presence and nature of the identification, authentication, and authorization mechanisms in place for the NSW will be discussed at length in Section D below. This section of the gap analysis will deal with:

(a) Over-arching policies that require security measures (among others, identification, authentication and authorization mechanisms); and
(b) The legal framework surrounding the privacy and confidentiality of NSW data.

78. The legal framework’s coverage of privacy issues, which for the purpose of this discussion correlates to the collection, storage, and processing of personally identifiable information, shall be covered extensively by the next section.

Data Protection Laws and Regulations

79. The ECA contains provisions directed towards protecting the integrity of information and communications systems and data contained therein. Section 33 of the ECA penalizes hacking or cracking, which is defined as:

a. The unauthorized access into or interference in a computer system/server or information and communication system; or

\textsuperscript{132} Recommendation No. 35 - Establishing a Legal Framework for International Trade Single Window (United Nations Economic Commission for Europe, December 2010), sec. 11.
\textsuperscript{133} Agreement to Establish and Implement the ASEAN Single Window, 2005, sec. 3.
\textsuperscript{134} Ibid., sec. 4.
\textsuperscript{135} Protocol to Establish and Implement the ASEAN Single Window, 2006, secs. 4–5.
b. Any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document.\(^\text{136}\)

80. Any of the above acts are punishable by a fine of at least one hundred thousand pesos (Php 100,000) and mandatory imprisonment of at least six months to three years.\(^\text{137}\)

81. The law also penalizes, among others, the unauthorized copying, distribution, alteration, or even storage of protected material, electronic signature, or copyrighted works.\(^\text{138}\) Although the provision is situated within the policy of protecting intellectual property, it may be broad enough to cover acts intended to breach NSW security or acts performed after such a breach. We note that some information submitted to the NSW may be treated as trade secrets or confidential information and thus fall under the ambit of “protected material”.

82. The Philippine legislature recently enacted a cybercrime law\(^\text{139}\) that punishes illegal access to computer systems, illegal interception of data, and data or system interference.\(^\text{140}\) The law likewise penalizes computer-related forgery, fraud, and identity theft.\(^\text{141}\)

83. The CPA mandates service providers to retain traffic data, subscription information, and even content data for a period of six months, extendable for another six months upon request of law enforcement.\(^\text{142}\) The law likewise allows real-time collection, even without a court warrant of data relating to a communication’s origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.\(^\text{143}\)

84. To date, petitions have been filed before the SC asking for the nullification of the law (or some of its provisions) on constitutional grounds.\(^\text{144}\) The SC has issued a temporary restraining order suspending the effectivity of the law for 120 days.\(^\text{145}\)

\(^{136}\) ECA, sec. 33(a).
\(^{137}\) Ibid.
\(^{138}\) Ibid., Section 33(b).
\(^{140}\) Ibid., sec. 4.
\(^{141}\) Ibid.
\(^{142}\) Ibid., sec. 13.
\(^{143}\) Ibid., sec. 12.
Oral arguments on the merits of the petitions are scheduled for January 15, 2013.

85. Recommendation 35, as well as other applicable information security standards, proceeds from the understanding that data protection and information security, for purposes of this gap analysis, cover not just the technological components, but also the presence of standards and practices for human agents.\textsuperscript{147}

86. Hence, beyond the security features already in place for the current PNSW implementation,\textsuperscript{148} there is a need to evaluate how the existing legal and regulatory framework of the PNSW addresses the need for data protection.

87. Rather than prescribe a specific suite of technological tools or strategies to maintain security, the ECA gives parties to a transaction the level of security of electronic documents they require.\textsuperscript{149}

88. The ECA mandates the government agencies which deploy electronic transaction systems to include “control processes and procedures…to ensure adequate integrity, security and confidentiality of electronic data messages or electronic documents or records or payments” in the transactions that they carry out.\textsuperscript{150}

89. The Philippines recently enacted the DPA.\textsuperscript{151} The new law is primarily oriented at protecting personal information\textsuperscript{152} and regulating entities that control and process such information. Nevertheless, the law provides some data protection and security-related provisions, such as requiring personal information controllers to:

   a. Implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing;

   b. Implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction,

\textsuperscript{146} Ibid.
\textsuperscript{147} Recommendation No. 35 - Establishing a Legal Framework for International Trade Single Window, secs. 11–12. The Recommendation frames data protection primarily in terms of controlling access by human agents.

\textsuperscript{148} The current NSW system is secured by requiring users (both trader-side users as well as government-side users) to go through a login mechanism. Login information includes password. After registration of their user names, users can authenticate themselves with the NSW system through a single factor: a password. See discussion on “Identification, Authentication, and Authorization” below for details on how user logins are generated.

\textsuperscript{149} Republic Act 8792, Electronic Commerce Act, sec. 24.
\textsuperscript{150} Ibid., sec. 27(d)(4).
\textsuperscript{151} Republic Act 10173, Data Privacy Act of 2012 (2012).
\textsuperscript{152} “Personal information” is defined in the DPA as “any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.” Ibid., sec. 3(g). The definition is substantially similar to that of “personal data” in the EU Privacy Directive.
and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination;

c. Ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision;

d. Ensure that their employees, agents or representatives who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations;

e. Promptly notify the privacy administration authority and affected data subjects when there is reason to believe that an unauthorized person has accessed personal information.153

90. According to the DPA, what security measures will be deemed reasonable shall be based on:

a) The nature of the personal information to be protected;
b) The risks represented by the processing;
c) The size of the organization and complexity of its operations; and
d) Current data privacy best practices and the cost of security implementation.154

91. Subject to guidelines from the privacy administering authority, the DPA provides a minimum set of security practices:

a. Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
b. A security policy with respect to the processing of personal information;
c. A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
d. Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.155

92. The PNSW MOA tasks the participating government agencies to comply with the agreement’s terms and conditions, which include information security

153 Ibid., sec. 20.
154 Ibid.
155 Ibid.
requirements. Provisions of the said MOA that may intersect with information security include:

- Observance of the confidentiality and secrecy of documents;
- Establishment of policies and regulations for sharing, use, and dissemination of data;
- Maintaining the security of their respective information systems; and
- Requiring entry into a “secure and updated” registry for users in all private and government entities that will access the NSW system.\(^{156}\)

93. To date, no requirements or guidelines on information and sharing mentioned in subparagraph (b) above have been enacted by the PNSW-SC or the PNSW-TWG. Neither have specific security measures or standards been adopted for the PNSW.

94. Nevertheless, to the extent that the participating government agencies have issued data security related regulations for their internal purposes or have expressly adopted or recommended well-defined information security standards for processes that intersect with the PNSW workflow, the same may be considered as part of the PNSW’s legal framework addressing data protection.

95. The BIR issues permits required by customs authorities. Its data activities therefore intersect with the PNSW workflow. Revenue Regulation (RR) 09-09, which governs the agency’s treatment of electronic records, is relevant in as far as the data submitted to or processed by the BIR will be the basis of processing in the PNSW. Under this regulation, taxpayers may develop their own data processing systems (subject to review and approval of the BIR) that will provide the basis for their tax information. Taxpayers who elect to develop such systems bear the responsibility of maintaining security and transaction integrity through measures that include:

- Access controls to ensure that only authorized users can have access to a computer system to process data;
- Input and output controls to ensure the accuracy and security of the information created, received, and transmitted;
- Processing controls that protect and ensure the integrity of the information processed by the system;
- Back-up controls that guarantee the retention of backup copies of electronic records in case of system failure;
- Controls to ensure that there is no accidental or intentional editing or deletion of recorded or completed transactions. Changes to any recorded transaction must be made by journal entry, be adequately documented, and include the following:
  
  i. Person making the modifications
  ii. Date of change;

---

iii. Previous transaction details;
iv. Current transaction details; and
v. Reason for the change or deletion.  

96. The BIR, in implementing electronic linkages with taxpayers subject to excise taxes, issued RR 05-02, which provides:

a. The treatment of taxpayer information with utmost confidentiality;
b. That the BIR shall institute sufficient security measures to prevent the destruction or hacking of their computer systems;
c. The exercise of security procedures to prevent divulgence of information to any unauthorized persons. 

97. For its internal information technology security arrangements, the BIR has developed its own Security Policies Manual as mandated by RMO 50-2004. The manual extensively covers a wide range of security arrangements, both from a technological viewpoint (network infrastructure, hardware management) to user-oriented concerns such as password management.

98. In implementing the Philippine EPCS, the EPCS Guidelines were enacted through a Joint Department Administrative Order by the DOF and the DTI. The EPCS Guidelines task the Government Electronic Payment and Collection System Evaluation Team (GEPCSET) to evaluate, accredit and recommend the adoption of EPCS systems for government entities. The order also provides that the EPCS should comply with the Philippine National Standards on Information Security Management System (ISMS) as approved by the BPS. The order lays down the following general areas as within the ambit of security standards:

a. Physical security measures and procedures to protect the EPCS, related electronic system and physical plant, and equipment from hazards and any unauthorized access and intrusions;
b. Technical security measures that protect the EPCS and its access control;
c. Administrative security procedures to provide for levels of access by select officials, personnel, and other persons authorized to access, maintain, develop, or inspect the EPCS; and
d. Independent vulnerability assessment shall be conducted for the EPCS prior to the launching of operations and periodically as may be

---

157 Revenue Regulation 09-09 - Maintenance, Retention, and Submission of Electronic Records, RR, 2009, sec. 5.5.
recommended by the GEPCSET. Results of such assessment should be favorable and acceptable to the GEPCSET.\textsuperscript{162}

99. Furthermore, the EPCS Guidelines provide that the EPCS implementations should comply with the DTI DAO No. 8. Although primarily concerned with privacy issues, it nevertheless provides general directives aimed at ensuring information security and managing agency risks between data controllers and data processors:

a. Implementation of appropriate organizational and technical measures intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the data to be protected and the risks represented by the processing and must be specified in a written document or its equivalent;

b. In case where data processing is contracted out, the data processor must provide guarantees in respect of adequate technical and organizational data protection measures and ensuring compliance with those measures;

c. When authorizing the data processor to process personal data, the data controller shall stipulate that personal data must be processed only on instructions from the data controller;

d. The relations between the data controller and the data processor who is not the data controller shall be regulated by a written contract except where such relations are provided for by laws or other legal acts; and

e. The employees of the data controller, the data processor and their representatives who are processing personal data must keep confidentiality of personal data if these personal data are not intended for public disclosure. This obligation shall continue even after their transfer to another position or upon termination of employment or contractual relations.\textsuperscript{163}

100. The ISO/IEC 27000:2009 series of standards for information security, which was adopted by the BPS, propose the setting up of a permanent ISMS through the following processes:

a. Identifying information assets and their associated security requirements;

b. Assessing information security risks;

c. Implementing relevant controls to manage unacceptable risks;

d. Monitoring, maintaining and improving the effectiveness of security controls associated with the organization's information assets.\textsuperscript{164}

\textsuperscript{162} Ibid., pt. VII(A)(3).

\textsuperscript{163} DTI Department Administrative Order No. 08-06 - Prescribing Guidelines for the Protection of Personal Data in Information and Communications System in the Private Sector, AO, 2006, sec. 8.

101. The ISMS contemplates an initial assessment stage where potential risks are identified, analyzed, and evaluated. At the same time criteria for accepting risks and identifying acceptable levels of risk are drawn to guide how the organization can act on such risks. Options for action include:

   a. The application of appropriate controls;
   b. Acceptance of risks, provided it is compliant with the organization’s policies and risk-acceptance criteria;
   c. Risk avoidance
   d. The transfer of risk to other parties (e.g., insurers and suppliers).  

102. The current PNSW implementation features a suite of security features: a) a login system with a single secure factor (a password known to the user) supported by b) an online registration system that relies on the submission of paper-based credentials and personal appearance before the PNSW’s registration authority. Access to the system, as well as assignment of available transaction privileges, is managed through an access control list.

103. These provisions notwithstanding, this gap analysis proceeds from the understanding that data protection and information security cover not just the technological components but also the presence of standards and practices for human agents and organizations. We take note that in some high-profile cases of information security breaches, the attack vector involves "social engineering", i.e. the manipulation of individuals or organizations in order to obtain confidential information. It is thus important to act not just on the technological arrangements of a system but the overlay of rules that guide human behavior on their use.

104. Legal provisions punishing actors engaged in breaching data systems, when coupled with a robust system for enforcement (detection, apprehension, and imposition of penalties), are important albeit partial components of a comprehensive approach to information security. The threat of criminal sanctions can change the cost-benefit analysis of those contemplating compromising the PNSW system’s security and can serve as a strong deterrent against security breaches. However, pursuing criminal sanctions for each breach would involve a significant investment given the high evidentiary requirements of securing a conviction.  

105. Given the effort and expense required for securing criminal convictions, the legislature may consider giving the PNSW implementing agency the power to vindicate administrative and civil sanctions against offenses to the NSW’s data protection and information security interests.

106. Beyond punitive measures, the PNSW-SC, as well as the participating government agencies, should consider adopting affirmative measures for the continuous evaluation and improvement of security based on widely accepted international standards.

---

165 Ibid., pt. 4.2.1.
166 The ROC requires proof “beyond reasonable doubt” to secure conviction.
<table>
<thead>
<tr>
<th>Gaps and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given the effort and expense required for securing criminal convictions, the legislature may consider giving the PNSW implementing agency the power to vindicate administrative and civil sanctions against offenses to the NSW’s data protection and information security interests.</td>
</tr>
<tr>
<td>Beyond punitive measures, the PNSW-SC, as well as the participating government agencies, should consider adopting affirmative measures for the continuous evaluation and improvement of security, based on widely accepted international standards.</td>
</tr>
<tr>
<td>Such measures should be applicable not only to private parties, but mandatory upon government agencies that receive and process NSW-related information. PNSW legislation should provide a precise timeline for the implementation of these security measures, and provide as well for consequences for failure to adopt them, whether at the agency level (for failing to issue and circulate implementing rules adopting security measures) the level of the individual employee (failure to comply with specific security measure). As in active efforts to breach PNSW security above, such omission-based offenses may be dealt with through a choice of criminal, civil, or administrative sanctions.</td>
</tr>
<tr>
<td>To date, neither the PNSW-SC nor the PNSW-TWG has issued detailed guidelines covering the issue of data protection or information security. In the absence of existing legal standards for the implementation of security practices in the PNSW, the PNSW-SC or the PNSW-TWG may adopt well-accepted international standards related to data protection or information security. In assessing the measures to be adopted, the PNSW-SC may adopt the works of scientific and other expert bodies.</td>
</tr>
<tr>
<td>ISO/IEC 27000:2009 (or some of its components) may be considered in drafting security standards for the PNSW. At the minimum, the PNSW-SC should consider adopting the ISMS approach, establishing a permanent security apparatus to its operations to not only implement security controls but to engage in the continuous review and assessment of the PNSW’s security.</td>
</tr>
<tr>
<td>Should national legislation be enacted to formalize a PNSW authority, such agency should be sufficiently empowered to promulgate or adopt relevant data protection standards that are applicable to both the public and private sectors.</td>
</tr>
<tr>
<td>In the meantime, the participating government agencies may issue joint agency guidelines on operational security. Such guidelines should</td>
</tr>
</tbody>
</table>
move beyond laying down mere references to or general principles on data protection and information security, or simple non-disclosure agreements, but codify a set of specific practices and procedures that can be carried out regularly. The guidelines should be translated into system-ready business rules that can be ported to the ASW environment.

- Furthermore, the foregoing guidelines should cover not only the technological components of the security picture but also its organizational aspects as well. The DPA and the DTI AO 8, including the BIR RR-09-09 may guide the participating government agencies as to the coverage of data protection policies.

Privacy and Treatment of Confidential Information

107. Privacy, as well how proprietary and confidential business data are protected, is an issue closely tied to that of data protection.\textsuperscript{167} Recommendation 35 states that NSW facilities should be compliant “with all relevant data protection laws”.\textsuperscript{168} See the discussion on “Access to and Sharing of NSW Data” for a more extensive treatment of the Philippines’ legal framework for the recognition and protection of privacy rights.

108. Recommendation 35 notes that although there is as yet no universal definition of privacy, several models are available from which national measures can be based on. The approaches considered in this gap analysis include:

a. The APEC Privacy Framework;

b. The OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data; and

c. The EU Data Protection Directive.

109. Although these standards may diverge as to the precise coverage of privacy rights, the common thread is that they cover some or all of the following areas of concern:

a. Defining what kind of data is subject to protection (i.e. private data, personal data, confidential data);

b. Defining actors in the protected data processing chain (i.e. data controllers, data processors, and data subjects);

c. Defining the rights and obligations of data controllers;

\textsuperscript{167} Recommendation No. 35 - Establishing a Legal Framework for International Trade Single Window, sec. 12.

\textsuperscript{168} Ibid.
d. Setting the rights of data subjects;
e. Laying down principles for determining allowable access to and
   processing of personal data; and
f. Describing a system for the enforcement of the rights of data subjects.

110. The DPA generally tracks these areas of concern, setting up a new agency
tasked to oversee compliance by both the private and public sectors to the
requirements of the law: The DPA’s policy declaration maintains that it springs
from a legislative intent of ensuring that “personal information…in the government
and in the private sector are secured and protected.”169 Likewise, the DPA allows
the privacy administering authority to monitor government compliance170 and even
“compel or petition any entity, government agency or instrumentality to abide by
its orders or take action on a matter affecting data privacy.”171

111. The DPA creates two tiers of protection: one for personal information172 and
another for privileged173 and sensitive personal information.174 While the collection
and processing of personal information are generally allowed subject to basic
requirements of the DPA, privileged and sensitive information cannot be
processed at all save for exceptional circumstances.

112. Participating government agencies are subject to the requirements in Sections 22
to 24 of the DPA when it comes to processing personal data. Section 23 requires
government employees to obtain a security clearance from the head of the agency
where the data originate prior to any on-site or online access to sensitive personal
information. Off-site access to sensitive personal information is prohibited unless
approved by the head of the agency, limited to a thousand records and encrypted
under “the most secure encryption standard”.175

170 Ibid., sec. 7(d).
171 Ibid., sec. 7(e).
172 Section 2(g) of the DPA defines personal information as “any information whether recorded in a
material form or not, from which the identity of an individual is apparent or can be reasonably and
directly ascertained by the entity holding the information, or when put together with other information
would directly and certainly identify an individual.”
173 Section 2(k) of the DPA defines privileged information as “any and all forms of data which under the
Rules of Court and other pertinent laws constitute privileged communication.”
174 Section 2(l) creates a subset of personal information that is:
   "(1) About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or
   political affiliations;
   (2) About an individual’s health, education, genetic or sexual life of a person, or to any proceeding for
   any offense committed or alleged to have been committed by such person, the disposal of such
   proceedings, or the sentence of any court in such proceedings;
   (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social
   security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation,
   and tax returns; and
   (4) Specifically established by an executive order or an act of Congress to be kept classified."
175 Republic Act 10173 - Data Privacy Act of 2012, sec. 23(b).
113. The law includes a textual reference to the EU Data Protection Directive’s chief principles of “transparency, legitimate purpose, and proportionality”. As will be discussed below, the rest of the DPA closely tracks the language of the EU Directive.

114. It should be noted that unlike the APEC Framework, the DPA does not require a nexus between collection and processing limitations and the risk of harm that may result from the misuse of personal information. The DPA’s prescriptions on collection and processing are applicable independent of the controller’s or data subject’s subjective evaluation of the likelihood of harm.

115. Notice - An individual has the right to know when collection of personal information is being performed. Such personal information should be “[c]ollected for specified and legitimate purposes”. Such notice should be given “before, or as soon as reasonably practicable after collection”. The data subject should likewise be informed when his personal information “shall be, are being or have been processed.” Further processing should be “compatible with such declared, specified and legitimate purposes only”. Notice prior to entry in the information controller’s system of the should include:

   a. Description of the personal information to be entered into the system;
   b. Purposes for which they are being or are to be processed;
   c. Scope and method of the personal information processing;
   d. The recipients or classes of recipients to whom they are or may be disclosed;
   e. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
   f. The identity and contact details of the personal information controller or its representative;
   g. The period for which the information will be stored; and
   h. The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

116. Right to opt-out – A data subject has the right to “[s]uspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller’s filing system” if such personal information are

---

176 Ibid., sec. 11.
177 Part III, Principle I of the APEC Framework: “Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.”
179 Ibid.
180 Ibid., sec. 16(a).
181 Ibid., sec. 11(a).
182 Ibid., sec. 16(b).
“incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected.” 183

117. **Legitimate purpose** – Personal information may only be collected, processed for legitimate purposes. 184 The information shall likewise be retained for as long as necessary to carry out such legitimate purpose. 185 Personal information may be lawfully processed when at least one of the following conditions exist:

a. The data subject has given his or her consent;
b. The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
c. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
d. The processing is necessary to protect vitally important interests of the data subject, including life and health;
e. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
f. The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution. 186

118. **Security** – As discussed in the section on data protection, the personal information controller should implement appropriate technical and organizational measures to protect personal data. The measures must be appropriate to the risks represented by the processing and the nature of the data be protected.

119. **Rectification and Amendment** – The data subject has the right to dispute inaccurate or erroneous information and have the information controller correct the same. 187

120. **Enforcement** – The DPA provides for mechanisms for data subjects to seek legal relief for violations of their privacy rights.

121. **Extraterritoriality** - The DPA also contains a set of provisions which will expand the applicability of the DPA's prescriptions to collection or processing performed outside the country given a sufficient nexus with the local jurisdiction, as may be demonstrated by the following circumstances:

---

183 Ibid., sec. 16(e).
184 Ibid., sec. 11(a).
185 Ibid., sec. 11(e).
186 Ibid., sec. 12.
187 Ibid., sec. 16(d).
a. The act, practice or processing relates to personal information about a Philippine citizen or a resident;

b. The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:

   i. A contract is entered in the Philippines;
   ii. A juridical entity unincorporated in the Philippines but has central management and control in the country; and
   iii. An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

c. The entity has other links in the Philippines such as, but not limited to:

   i. The entity carries on business in the Philippines; and
   ii. The personal information was collected or held by an entity in the Philippines.188

122. The DPA does not cover nor protect personal information “originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws”.189

Gaps and Recommendations

- Each participating government agency as well as any future PNSW administering entity would function as a personal information controller. Other entities in the PNSW processing chain, whether private or public, may be considered personal information processors under the law. The participating government agencies must re-align their data collection and processing to conform to the provisions of the DPA. This can be carried out not just by issuing administrative rules on the collection and processing of personal information but also by including the DPA’s requirements into the contracts it enters into with service providers. Compliance studies may be conducted to determine the extent to which each participating agency’s processes and standards would need to be reconfigured in order to comply with both the DPA and its obligations to the ASW initiative.

- The DPA will need to closely coordinate with the newly created NPC in developing the network of internal policies and contracts to make sure that the same is compatible with the DPA and its implementing rules.

188 Ibid., sec. 6.
189 Ibid., sec. 4(g).
Gaps and Recommendations

- At the same time, the PNSW should develop user-facing components of a privacy regime required by the DPA:
  - A user-oriented privacy policy, which should be shown to the user prior to collection of personal information;
  - A system for notifying the user pursuant to section 16 of the DPA (i.e. when personal information has been processed, purpose of the processing, etc.);
  - Provisions for rectifying and amending personal information.

- Participating government agencies should take note that for any given user submission for processing, even when facilitated through a single form, some fields may contain sensitive personal information and therefore require different treatment under the DPA. Processing may be performed on both classes of data in the submission provided the data subject is given prior consent. In all cases (i.e. whether sensitive personal info or not), consent for disclosed uses is subject to the provisions of Section 11.

- No administrative issuances from the participating government agencies commit to exempting trade secrets or other proprietary information from the system’s disclosure requirements or attaching the condition of confidentiality in exchange for their disclosure.

- The DPA’s extraterritoriality provisions may complicate the PNSW’s interactions with the ASW or any other arrangement for the cross-border movement of information that involve data with a Philippine nexus. The OECD Guidelines urge Member countries to “refrain from restricting cross-border flows of personal data between itself and another Member country”, save only for cases where the other jurisdiction has failed to substantially comply with the guidelines or where the transmission will result the circumvention of domestic legislation. The EU Data Protection Directive also restricts cross-border flows of personal information to countries that do not provide a similar level of protection. Given that the DPA does not protect the personal information of non-residents, then cross-border flow of data from the EU and for that matter other ASW Member States that have adopted privacy laws that hew closely either to the EU or OECD models will be impeded.

- The DPA’s extraterritoriality provision extends the law’s prescriptions overseas so long as a nexus to the Philippines may be established. Notably, personal information controllers such as PNSW participating government agencies should take note that for any given user submission for processing, even when facilitated through a single form, some fields may contain sensitive personal information and therefore require different treatment under the DPA. Processing may be performed on both classes of data in the submission provided the data subject is given prior consent. In all cases (i.e. whether sensitive personal info or not), consent for disclosed uses is subject to the provisions of Section 11.

---

191 Ibid.
agencies, are accountable for violations of the DPA even by off-shore third party processors, such as ASW Member States’ NSWs. The threat of liability under the DPA may therefore limit the degree to which the PNSW would be willing to pass on personal information to the ASW. This would have an adverse impact on the PNSW’s integration into other national or regional facilities.

- It is recommended that the NPC be empowered to manage the balance between the need to maintain privacy as well as facilitate information sharing, and efficiency for cross-border transmission of personal information. This may be done by amending the law to allow the Government to carve exceptions to the applicability of the DPA’s provisions (as to cross border transmissions) based on executive agreements; or the PNSW can coordinate with the NPC for a favorable opinion or ruling. Alternatively, in consideration of the cross-border requirements of the PNSW, the law may define a different policy data policy regime applicable to PNSW data, or an administrative mechanism for resolving cross-border data protection issues based on executive agreements or reciprocity.

### C. Access to and Sharing of NSW Data

123. Article I of the ASW Agreement and the ASW Protocol refer to the NSW as a system that enables, *inter alia*: (1) a single submission of data and information; and (2) a single and synchronous processing of data and information. For this purpose, the ASW Protocol to the ASW Agreement states that data and information shall be submitted, collected and processed in an agreed format and transmitted through secured channels and in established communication and interface protocols as defined by Member Countries. The ASW MOU, on the other hand, refers to the ASW as constituting a regional facility to enable a seamless, standardized and harmonized routing and communication of trade and customs related information and data for customs clearance and release from and to NSWs.

124. From the foregoing, therefore, it is immediately apparent that access to and sharing of information between and among NSWs, NSW participating government agencies and users are paramount and integral components of the ASW and NSW system, such that the ASW MOU emphasizes the significance for member states to study and identify the requirements of an adequate legal framework to enable operations of the ASW that will permit cross-border exchange of data and documents, and where appropriate, establish policies and

---

192 DPA, sec. 21.  
193 ASW Protocol, art.7(1).  
194 ASW MOU, art.I(1).
regulations, and develop Memoranda of Understanding and/or Interconnection Security Agreements for the sharing, use, and dissemination of data and information, not only for the domestic government usage, but also for the mutual recognition of such data and information of other NSWs being communicated within the ASW.\textsuperscript{195}

125. In any discussion of sharing and access of information, it is inevitable to consider privacy and confidentiality issues, which fact has been recognized in both the ASW Protocol and the ASW MOU. The ASW Protocol specifically states that access to, exchange, use, legal validity, and confidentiality of data and information in the framework of the ASW are subject to the national laws and regulations of the respective Member Countries,\textsuperscript{196} whereas, the ASW MOU devotes special articles on confidentiality\textsuperscript{197} and privacy of data.\textsuperscript{198} The ASW MOU essentially obligates each ASEAN Member State to: (1) observe the confidentiality and secrecy of documents, information and other data received from, or supplied to other ASEAN Member States;\textsuperscript{199} (2) protect confidential information including sensitive and personally identifiable information, and trade-sensitive information about companies participating in the ASW and NSW from unlawful access, use and disclosure;\textsuperscript{200} (3) establish in agreements between any of the member states, if necessary, limitations on sharing of data and information;\textsuperscript{201} (4) require that data and information which are furnished by a trader to its NSW be transmitted to another NSW only with the prior consent of the trader;\textsuperscript{202} and (5) require that authorized registered users of its NSW shall not be permitted access to information or data other than those information or data for which access has been authorized by law or regulation.\textsuperscript{203}

126. Recommendation 35 recognizes that establishing a NSW requires a complex process that necessarily includes a careful assessment of existing laws, regulations, and practices governing the flow of trade-related information,\textsuperscript{204} and the identification of existing and potential barriers related to trade data exchange.\textsuperscript{205} Questions pertaining to when and how data may be shared and under what circumstances and with what organizations within the government or with government agencies in other countries and economies would have to be addressed.\textsuperscript{206} Pursuant to this, Recommendation 35 suggests that governments should establish, if there are none existing, policies and regulations regarding the use of data, such as retention, confidentiality, privacy, redistribution or

\begin{itemize}
  \item \textsuperscript{195}Ibid., art.XI(1),(2).
  \item \textsuperscript{196}ASW Protocol, art. 7(4).
  \item \textsuperscript{197}ASW MOU, art. VIII.
  \item \textsuperscript{198}Ibid., art. XII, see also art. IX(4).
  \item \textsuperscript{199}Ibid., art. VIII(1).
  \item \textsuperscript{200}Ibid., art. XII(1), (2).
  \item \textsuperscript{201}Ibid., art. IX(5).
  \item \textsuperscript{202}Ibid., art. IX(6).
  \item \textsuperscript{203}Ibid., art. XII(3).
  \item \textsuperscript{204}Recommendation 35, sec. 4.
  \item \textsuperscript{205}Ibid., sec. 5.
  \item \textsuperscript{206}Ibid., sec. 7.
\end{itemize}
sharing.\textsuperscript{207} In the aspect of privacy, Recommendation 35 invites attention to a consideration of how and under what circumstances access to data provided to the NSW should be authorized both nationally and with other NSWs, noting that some countries operating NSWs have developed a MOU type of approach in this area for the exchange of data between them.\textsuperscript{208} It is likewise pointed out by Recommendation 35 and required of member countries in both the ASW Protocol\textsuperscript{209} and the ASW MOU\textsuperscript{210} that these bilateral or multilateral agreements, as well as, the internal rules for accessing data within the NSW should comply with international standards and harmonized to the greatest extent possible.\textsuperscript{211}

127. Considering that what is being contemplated by the ASW is an electronic NSW system, Recommendation 35 indicates that it is also important for member states to review their respective general legal framework for electronic commerce, including electronic communications.\textsuperscript{212}

128. This section shall assess the existing legal framework in the Philippines in relation to the access and sharing of information, consisting of laws, regulations, and jurisprudence enabling access and sharing of information, and those which serve to restrict or limit the same, such as those with respect to privacy and confidentiality of certain classes of information.

**Philippine Legal Framework Relevant to Access to and Sharing of Information**

129. While there is no provision in the Philippine Constitution (“Constitution”) directly promoting or enabling information sharing and access thereto, Article II, Section 24 of the Constitution provides that the “State recognizes the vital role of communication and information in nation-building.” Meanwhile, Article XVI, Section 10 of the Constitution makes it a policy of the state to provide an “environment for the full development of Filipino capability and the emergence of communication structures suitable to the needs and aspirations of the nation and the balanced flow of information into, out of, and across the country, in accordance with a policy that respects the freedom of speech and of the press.” This, in a broad sense, therefore, encourages communication or exchange of information within and out of the country, subject of course, to limitations that may be found in the Constitution itself, and laws and regulations restricting the same, as will be discussed hereunder.

130. For purposes of this discussion, it is imperative to identify the different classifications of data and information and be able to distinguish what kind of information may be shared and accessed and the manner in which these information is allowed or restricted to be accessed and shared, based on Constitutional, statutory, and jurisprudential guidelines.

\textsuperscript{207}Ibid., sec. 12.  
\textsuperscript{208}Ibid.  
\textsuperscript{209}ASW Protocol, art.7(2),(3).  
\textsuperscript{210}ASW MOU, art. VI.  
\textsuperscript{211}Recommendation 35, sec.12.  
\textsuperscript{212}Ibid., sec. 7.
Information and data can first be classified into public and private. As a general rule, public information on matters of public concern and those involving public interest can be accessed, in accordance with Article II, Section 28 and Article III, Section 7 of the Constitution, thus:

“Sec. 28. Subject to reasonable conditions prescribed by law, the State adopts and implements a policy of full public disclosure of all its transactions involving public interest.”

“Section 7. The right of the people to information shall be recognized. Access to official records, and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law.”

Jurisprudence, however, states that the right to public information does not extend to matters recognized as privileged information under the principle of separation of powers,213 and that the right does not also apply to information on military and diplomatic secrets, information affecting national security, and information on investigations of crimes by law enforcement agencies before the prosecution of the accused, which courts have long recognized as confidential.214 Moreover, it has been held by the Supreme Court that the constitutional right to public information also includes official information on on-going negotiations before a final contract, but the information must constitute definite propositions by the government and should not cover recognized exceptions as mentioned above.215

Quite the opposite, as regards private information, as will be explained, the general rule is that it may not be accessed, much less, shared without the consent of the information or data subject, save for cases allowed by law or the Constitution. This is largely based on the Constitutional principles upholding the right of individuals to privacy. The right to privacy is guaranteed under Article III, Sections 2 and 3 of the Constitution, to wit:

“Section 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

Section 3.

213Chavez vs. PEA, G.R. No. 133250, 9 July 2002.
214Ibid.
215Ibid.
1. The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.

2. Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding."

134. It is submitted that the foregoing Constitutional provisions are wide enough to cover not only physical privacy, but also decisional and informational privacy. Although the latter two categories are not immediately apparent from the just stated provisions of the Constitution, guidance may be had from both Philippine jurisprudence and decisions of the United States Supreme Court, which have persuasive effect in our jurisdiction.

135. The case of Morfe v. Mutuc first recognized the constitutional right to privacy in its Philippine context where the Supreme Court emphasized the significance of privacy by declaring that the right to be let alone is “indeed the beginning of all freedom.” This pronouncement echoes the formulation made by Justice Brandeis in Olmstead v. United States that the right to be let alone was the most comprehensive of rights and the right most valued by civilized men.

136. Decisional privacy, which refers to the interest in independence in making certain kinds of important decisions, was recognized in Estrada v. Escritor, although the majority opinion dealt extensively with the claim of religious freedom, the separate opinion made reference to the decisional privacy aspect of the issue involved. In Griswold v. Connecticut, the US Supreme Court resolved a decisional privacy claim by striking down a statute that prohibited the use of contraceptives by married couples; in Meyer v. Nebraska, the US Supreme Court pronounced that the liberty guaranteed by the Fourteenth Amendment denotes not merely freedom from bodily restraint, but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, among others, and generally to enjoy those privileges essential to the orderly pursuit of happiness by free men; in Roe v. Wade, the US Supreme Court justified abortion in the United States on the premise that the

---

218 Supra, note 223.
219 277 U.S. 438 (1928).
220 Supra, note 223.
221 Ibid.
223 Supra, note 223.
224 381 U.S. 479 (1965).
225 262 U.S. 390 (1923).
right of privacy is broad enough to encompass a woman’s decision whether or not to terminate her pregnancy; and in *Lawrence v. Texas*, the US Supreme Court invalidated a law prohibiting sexual intercourse between consenting individuals of the same sex on the ground that individual decisions concerning the intimacies of physical relationships, even when not intended to produce offspring, are a form of “liberty” protected by due process.

137. Informational privacy, which refers to the interest in avoiding disclosure of personal matters, on the other hand, has been said not to be absolute and should be counterbalanced against the State’s interest in acquiring or disclosing the information. In the US, it has been observed that majority of the US Courts have required a showing from the government that a substantial interest for intruding into an individuals’ right to confidentiality in their personal information, and thereafter, balance the same against the individual’s interest in confidentiality. This type of balancing test originated from *United States v. Westinghouse*, taking into consideration several factors, namely: (a) the type of record requested; (b) the information it did or might contain; (c) the potential for harm in any subsequent non-consensual disclosure; (d) the injury from disclosure to the relationship in which the record was generated; (e) the adequacy of safeguards to prevent unauthorized disclosure; (f) the degree of need for access; and (g) the presence of an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.

138. In the case of *Ople v. Torres*, the Supreme Court struck down as an invasion of the right to privacy an Administrative Order issued by the President of the Philippines, which Administrative Order provides for a Population Reference Number (PRN) as a “common reference number to establish a linkage among concerned agencies” through the use of “Biometrics Technology” and “computer application designs.” The Supreme Court ruled in the said case that the right to privacy does not bar all incursions into the right to individual privacy, but that the government failed to show that a compelling interest justify such intrusions, which intrusions must be accompanied by proper safeguards and well-defined standards to prevent unconstitutional invasions. According to the Supreme Court, the government likewise failed to show that the law is narrowly focused and neither broad nor vague, such that there is a clear and present danger to the people’s right to privacy. Specifically, the Supreme Court observed that while the methods or forms of biological encoding under the Administrative Order include finger-scanning and retinal scanning, as well as the method known as the “artificial nose” and the thermogram, the Administrative Order does not state what

---

227 Supra, note 223.
228 539 U.S. 558.
229 Supra, note 223.
230 Ibid.
231 Ibid.
232 638 F2d 570 (3d Cir 1980).
233 Supra, note 223.
235 Ibid.
236 Ibid.
specific biological characteristics, what particular biometrics technology shall be used, whether encoding of data is limited to biological information alone for identification purposes, nor does it indicate any assurance that personal information which will be gathered will only be processed for unequivocally specified purposes.237

139. In another ruling,238the Supreme Court upheld the validity of EO 420, which required all government agencies/GOCCs to adopt a uniform data collection and format for their IDs. Under EO 420, government entities can collect and record only fourteen (14) specific data mentioned in Section 3 of EO 420, which include, among others, a person’s name, address, sex, photo, signature, date and place of birth, civil status, physical attributes, and Tax Identification Number.

140. Another past experience is the establishment of a shared government information system for migration, as provided for in R.A. No. 8042. Such law called for the creation of an interagency committee composed of the DFA, DoT, DoJ, Immigration, DILG, etc. The committee was allowed to access the information contained in the respective agencies’ databases/files.

141. Consistent with the great significance accorded to the protection of the right to privacy, the Supreme Court has issued special rules to govern petitions for habeas data ("Habeas Data Rules").239Section 1 of the Habeas Data Rules defines the writ of habeas data as a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party. Decisions240of the Supreme Court have, however, limited the coverage of the writs to the protection of rights to life, liberty and security, and to cases of "extra-legal killings" and "enforced disappearances." These writs therefore, have little or no significance to data and information in the PNSW and ASW – both of which involve "commercial activities" for which the Court will not issue either writ.

The Data Privacy Act of 2012

142. Congress recently enacted the DPA, with the avowed policy to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth; and to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.241

---

237Ibid.
239A. M. No. 08-1-16-SC. 22 January 2008.
241DPA, sec. 2.
143. The DPA covers processing of all types of personal information and defines the term “processing” as referring to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

144. The DPA, however, enumerates certain types of information that are not covered by its application, thus:

“(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

(1) The fact that the individual is or was an officer or employee of the government institution;

(2) The title, business address and office telephone number of the individual;

(3) The classification, salary range and responsibilities of the position held by the individual; and

(4) The name of the individual on a document prepared by the individual in the course of employment with the government;

(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;

(d) Personal information processed for journalistic, artistic, literary or research purposes;

(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Note that the DPA states that nothing in the said law shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign...
Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or BSP to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and

(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.”

145. The DPA applies to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines.\footnote{Ibid., sec. 4.} The term “personal information controller” is defined in the DPA as a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf.\footnote{Ibid., sec. 3(h).} The definition excludes: (1) a person or organization who performs such functions as instructed by another person or organization; and (2) an individual who collects, holds, processes or uses personal information in connection with the individual’s personal, family or household affairs.\footnote{Ibid.}

146. It is noted that the DPA makes no distinction between, and therefore applies to both, public and private information controllers. Moreover, the DPA has an extra-territorial provision that makes the law applicable to persons or entities even outside Philippine territory, provided that the act done or practice engaged in by an entity in violation of the law, whether done within or without the Philippines, relates to personal information about a Philippine citizen or a resident, and the entity has a link with the Philippines.\footnote{Ibid., sec. 6.} This provision will be discussed at length in the section on Legal Liability and Dispute Resolution.

147. Two types of personal information are contemplated in the DPA, namely: (1) personal information; and (2) sensitive personal information, respectively enjoying varying degrees of protection, as will be discussed in the succeeding paragraphs. Personal information under the DPA comprehends any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and
certainly identify an individual. Sensitive personal information, on the other hand, refers to personal information:

“(1) About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(2) About an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.”

As for personal information, the DPA states the rule that processing thereof is allowed, subject to compliance with the requirements set forth in the said law, as well as other laws allowing disclosure of information to the public. The DPA further states that personal information must be:

“(a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

(b) Processed fairly and lawfully;

(c) Accurate, relevant and, where necessary for purposes for which it is to be used, the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

(d) Adequate and not excessive in relation to the purposes for which they are collected and processed;

(e) Retained only for as long as necessary for the fulfilment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

249 Ibid., sec. 3(g).
250 Ibid., sec. 3(l).
251 Ibid., sec. 11.
(f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing.”

149. To allow the lawful processing of personal information, the DPA provides, as follows:

“SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

(a) The data subject has given his or her consent;

(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.”

252Ibid.
253Ibid., sec. 12.
150. In contrast, the DPA expressly states that in the case of sensitive personal information and privileged information, processing is prohibited save in specific cases, as follows:

“(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

(b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

(d) The processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.”

151. Accordingly, the DPA gives certain right to data subjects, defined as an individual whose personal information is processed, which include the rights to:

(a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;

(b) Be furnished the information regarding the description, purpose, scope, recipients, method of access (when allowed), identity and contact details of the personal information controller, retention period, and data subject rights, before the entry of his or her personal information into the

---

254 DPA, Section 3(k) defines privileged information as any and all forms of data that under the ROC and other pertinent laws constitute privileged communication.

255 DPA, sec. 13.

256 Ibid., sec. 3(c).
processing system of the personal information controller, or at the next practical opportunity;

(c) Reasonable access to, upon demand, the contents, sources, names of recipients, manner by which data were processed, information on automated process, reasons for disclosure, date of access or modification, designation and identity of the personal information controller;

(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable, and have third parties who have previously received such processed personal information be informed of its inaccuracy and its rectification;

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller’s filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.257

152. The data subject shall also have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject.258

153. The DPA likewise imposes criminal liability for certain acts, namely: (1) unauthorized processing of personal and sensitive information; (2) accessing personal and sensitive information due to negligence; (3) improper disposal of personal and sensitive information; (4) processing of personal and sensitive information for unauthorized purposes; and (5) unauthorized access or intentional breach of personal information systems.259

257 Ibid., sec. 16.
258 Ibid., sec. 18.
259 Ibid., secs. 25-35.
154. To implement the law, the DPA creates a separate agency to be known as the National Privacy Commission ("NPC") with the authority, among others, to:

a. Implement the DPA and ensure compliance of personal information controllers with the DPA;

b. Monitor and ensure compliance of the country with international standards set for data protection;

c. Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers, which privacy codes shall adhere to the underlying data privacy principles embodied in the DPA;

d. Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;

e. Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;

f. Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws; and

g. Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations.

155. Given the above provisions of the DPA, it is believed that the following observations are material to the access and sharing of information in the context of the PNSW and the ASW:

a. The processing of personal and sensitive personal information is regulated by the DPA. Such information can be used only in accordance with the principles set out in its Section 11. This provision actually limits the lawful processing of all personal information.

b. The DPA in Section 4(e) expressly provides that it does not apply to information necessary in order to carry out the functions of public authority. This could conceivably be a justification for excluding the PNSW operations from the

---

260 Ibid., sec. 7.
261 The other functions and powers of the NPC are discussed in other sections of the Gap Analysis, where they may be more relevant.
262 Ibid., sec. 4(e).
coverage of the law but the DPA is inconsistent on the issue of
government-controlled data.

There seems to be conflicting provisions relating to personal
information handled by government. While Section 4(e)
appears to exclude all data necessary for public authority, all
personal information issued by government agencies are
considered sensitive personal information. Indeed, Sections 22
to 24 of the DPA treats of government processing of sensitive
personal information.

Because of the apparent conflict it might be that government
agencies would still have to comply with the DPA despite the
express mention that the DPA does not apply to information
necessary in order to carry out the functions of public authority
under Section 4(e) thereof.

It is suggested that the matter be raised with the NPC so it can
articulate a consistent policy on this matter.

c. The DPA does not apply to personal information originally
collected from residents of foreign jurisdictions.263This means
that these data may be processed without threat of criminal
prosecution. More to the point, this recognizes that foreign
citizens enjoy only a limited right of informational privacy in the
Philippines. ASW Member States and other NSWs therefore
may not be able to complain in the Philippines if the data of
their citizens collected abroad are exploited in the Philippines.

d. The DPA applies to entities even outside Philippine territory,
provided that the act done or practice engaged in by an entity
in violation of the law, whether done within or without the
Philippines, relates to personal information about a Philippine
citizen or a resident, and the entity has a link with the
Philippines.264 Moreover, a Philippine personal information
processor is accountable for the acts of parties to whom it
transfers such information, even if located off-shore265. PNSW
participating government agencies therefore may be
apprehensive about giving access to PNSW data for
processing through the ASW if they may be held accountable
for misdeeds done by third parties within ASEAN member
states.

e. It is further noted that when the PNSW processes data, it
must recognize that on a single form, some data fields are
sensitive and while others are not, in which case, the rules for

263Ibid., sec. 4(g).
264 Ibid., sec. 6.
265 Ibid., sec.21.
Consent for disclosed uses can address the situation but the PNSW will be constrained by the following:

(i) In all instances, whether sensitive personal information or not, consented use must conform to the DPA’s Section 11 principles. There appears to be no indication that this could be subject to stipulation or contract.

(ii) Regarding the manner in which the government will handle sensitive personal information under Sections 22 to 24, it should be noted that there is a requirement of a security clearance, yet the DPA does not provide the procedures or standards for the issuance of such security clearance.

f. Government contractors who process sensitive personal information relating to more than one thousand (1,000) individuals must register their data processing system with the NPC.266 In other words, a potential contractor of the PNSW system will have to comply with this provision.

Access to and sharing of information under Executive Order 482

156. The foregoing legal framework and principles would have to be considered together in the determination of rules and regulations on access and sharing of information in the NSW system.

157. EO 482 called for the formulation of guidelines meant to identify a common definition/ set of data, information, and processes for integration to the PNSW.267 Pursuant to the same, the BOC along with the participating government agencies entered into a Memorandum of Agreement for the Implementation of the PNSW dated 10 February 2012. These issuances, however, do not contain, as of yet, a specific set of rules and guidelines on the access and sharing of information among and between the NSW participating agencies. Neither is there any rule that specifically governs access and sharing of information among and between the NSW, ASW, and their users.

Other Laws and Issuances that may be Relevant to Access and Sharing of Information

158. The ECA-IRR says that relevant government agencies tasked with enforcing or

266 Ibid., sec. 24.
267 EO 482, sec. 6.
implementing applicable laws relating to the retention of certain documents may, by appropriate issuances, impose regulations to ensure the integrity, reliability of such documents. This means that the respective government agencies concerned are given the authority to determine and issue separate regulations to ensure the integrity, reliability, and hence, retention, of such documents.

159. Presidential Decree No. 1464, as amended, otherwise known as the Tariffs and Customs Code of the Philippines (“TCC”) requires customs officers to keep true, correct and permanent records of their official transactions, and to submit the same to the inspection of authorized officials at all times.268 In the specific instance of investigations concerning dumping, the TCC requires the BOC to notify the government of the exporting country about any impending antidumping investigation.269

160. Other than the afore-cited PNSW MOA among participating government agencies dated 10 February 2012, which is supposed to cover PNSW data, there are MOAs between a considerable number of government agencies for the sharing of data. For instance, there is a linkage between agencies under the DOF, such as the BIR and the BOC, for the purpose of information sharing.270 By virtue of this, the BIR regularly issues Letter Notices for Tax Deficiencies based on “Third Party Information” provided by the BOC. The BIR is also given the power, under R.A. 8424 or the National Internal Revenue Code (“Tax Code”), as amended, to obtain, on a regular basis from any office or officer of the national and local governments, government agencies and instrumentalities, any information such as, but not limited to, costs and volume of production, receipts or sales and gross incomes of taxpayers, and the names, addresses, and financial statements of persons, corporations, and other entities.271

161. Both the Tax Code and the TCC penalize the unauthorized divulgence of taxpayers’ records. Section 270 of the Tax Code prohibits the Unlawful Divulgence of Trade Secrets, while Section 278 of the same law penalizes any person who causes or procures an officer or employee of the Bureau of Internal Revenue to divulge any confidential information regarding the business, income or inheritance of any taxpayer, knowledge of which was acquired by him in the discharge of his official duties, and which it is unlawful for him to reveal. The only exception allowed by the Tax Code for access to taxpayer’s records is provided where there is an order from the President of the Republic of the Philippines.272 BIR Revenue Memorandum Order No. 50-2004 creates classifications of information under the custody of the BIR and imposes sanctions for the unauthorized processing thereof, in relation to BIR Revenue Memorandum Order No. 53-2010.

268 TCC, sec. 710.
269 Ibid., sec. 301 (d).
271 Tax Code, sec. 5 (b).
272 Ibid., sec. 71.
162. The TCC, on the other hand, considers it an offense, where, without authority of law, confidential information gained during any investigation or audit is disclosed or used.\(^{273}\)

### Gaps and Recommendations

- Other than the ASW Agreement and its protocol, there appears to be no law specifically mandating the BOC to coordinate and share information with other states.

- The PNSW MOA dated 10 February 2012 does not of itself provide definite guidelines on what information is to be shared within the PNSW and the ASW, what is to be considered as confidential information, the obligations and rights of the participating government agencies under the PNSW mechanism, the sanctions for non-compliance with the MOA, and a dispute resolution mechanism, among others. It would greatly help the establishment and use of the PNSW should another MOA or a supplemental MOA be entered into by the participating government agencies that would specifically and clearly address these issues, which guidelines should comply with national laws, particularly the DPA, as well as, international laws and standards.

- There appears to be no existing formal law that specifically mandates the allowable sharing of information across all government agencies. This should, of course, be consistent with the DPA. If possible, a law establishing the PNSW can specify the rules for the sharing and access of information for purposes of the PNSW and the ASW. It may provide for clear guidelines on what information will be provided to the PNSW, considering that access and sharing of information is a recognized exception to the general prohibition on the processing of personal and sensitive information.

- As suggested by Recommendation 35, periodic review of the impact of access and sharing of PNSW information or data on privacy and confidentiality considerations must be performed by the government.

- To the extent that access to PNSW data to local and foreign ASW stakeholders are regulated, the DPA regulates the processing and disclosure of data between government agencies and to third parties, and in that sense, data access is restricted.

- The DPA provides that it does not apply to information necessary in order to “carry out the functions of public authority.” The phrase, however, is not sufficiently defined in the law. This could, therefore, cause confusion, and worse, render the law inutile. It is suggested that the PNSW Task Force

---

\(^{273}\)TCC, sec. 3604.
require the NPC to issue a directive clarifying the law regulating government information.

- Considering the fact that the DPA does not apply to personal information originally collected from residents of foreign jurisdictions, and that under the law, Philippine personal information controllers are liable for acts done by third parties to whom personal information is transferred for processing, guidelines or agreements concerning access and sharing of information and protection to be afforded to information must be forged by ASW member countries for purposes of uniform protection and rights for all users.

- Rules and regulations as to the sharing and access of information or data can also be made part of end user agreements. These agreements must ensure that NSW users consent to the use or processing of data that they submit to the PNSW for the specific purpose of their transactions, as well as, other purposes that they may agree to. In turn, it should also be provided under these end user agreements that collected data will only be used for their intended purposes.

- Each PNSW participating government agency has to undertake a study of their personal data handling processes to ensure full compliance with the DPA.

### D. Identification, Authentication and Authorization

163. As mentioned above, technological methods for: (a) identifying and authenticating legitimate users of the PNSW; and, (b) authorizing operations and transactions based on these credentials, form components of the PNSW’s first line of security and hence, implicate data protection and privacy issues. Similarly, these components can link actions to specific actors and form the basis for a system of accountability and feedback. This, in turn, can guide a variety of regulatory actions.

164. Recommendation 35 relates to identification, authentication, and authorization mechanisms as a way to ensure the protection, quality, accuracy, and integrity of data in a NSW.\(^{274}\) The same likewise acknowledges that there is currently “no worldwide, legal, procedural standards covering this area”. NSW operators must rely on national law, taking into consideration emerging best practices and the requirements of interoperability.\(^{275}\)

\(^{274}\) Recommendation 35, sec. 13.

\(^{275}\) Ibid.
165. The OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication (OECD Authentication Papers) recognizes that authentication is a subsystem of larger security considerations, and defines the authentication, identification, and authorization problem as “a function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system”.276

166. The PNSW mechanism for identification, authentication, and authorization is implemented through the CPRS account, which is required prior to trader registration in the PNSW.277 The CPRS is a module of the e2m used to validate users and manage their access to a suite of e2m applications (e.g. Electronic Manifest System, Informal Entry System, Automated Bonds Management System, etc.).

167. The registration process and requirements for a CPRS account would depend on the prospective user’s “stakeholder type” based on a predefined set of categories.278 Importers are accredited by the CAS and the registration process involves the following steps:

a.Importer lodges his/her CPRS profile via the VASP (The importer must indicate his nominated broker by encoding his broker’s CCN.
b. The CAS receives the submitted accreditation application including required documents;
c. CAS performs approval of the submitted profile;
d. The CPRS will generate an email with attached Certificate of Registration indicating the assigned CCN for the broker as a proof of accreditation.

168. Though approval of the user registration is lodged with the CAS, three VASPs (Cargo Data Exchange Center, E-Konek Pilipinas, and Intercommerce Network Services)279 currently facilitate the process.

<table>
<thead>
<tr>
<th>Gaps and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Although the registration process is implemented in the PNSW and documented in the BOC or PNSW website, it has not been reduced into an over-arching policy supported by a formal legal framework. Beyond the technological components in place that enable the above functions, it is important not only to reflect government commitment to the accreditation</td>
</tr>
</tbody>
</table>

279 Ibid.
Gaps and Recommendations

mechanisms, but also to clarify the set of priorities involved in designing these mechanisms.

- It should be noted that the accreditation function not only involves traders, but also the employees of the regulatory agencies in the PNSW workflow. Likewise, in each leg of the PNSW workflow where the trader transacts to secure permits of a participating agency, the trader may be required to submit to a separate accreditation mechanism (i.e., the BIR will require submission and verification of the trader’s Tax Identification Number).

- The Philippines operates in what the OECD Authentication Papers describe as the sectoral or “siloh approach, where authentication mechanisms arise on an application-by-application basis, resulting in a proliferation of identification cards and accreditation processes.280

- Considering the number of participating government agencies involved and the volume of transactions requiring proof of identity, it may be appropriate to determine the commonalities across applications to arrive at a single identification system. Not only will this capture economies of scale, but will

280 BSP Circular 564 enumerates the following valid forms of identification for the banking sector:
1. Passport
2. Current Driver’s License ID
3. Permit to Carry Firearms
4. New Social Security System card (SSS ID)
5. Government Service Insurance System (GSIS) eCard
6. Professional Regulation (PRC) ID
7. New Tax Identification Number (TIN)
8. Postal ID
10. NSO authenticated Marriage Certificate
11. Original and Unexpired National Bureau of Investigation (NBI) Clearance
12. Police Clearance
13. Digitized Voter’s ID
14. Philhealth Card
15. Office of Senior Citizen’s Affairs (OSCA) / Senior Citizen’s Card
16. ACR Identity Card (I-Card)
17. Consular ID
18. Barangay Certificate
19. Philippine Overseas Employment Association (POEA)
20. Overseas Worker's Welfare Administration (OWWA)
21. OFW ID
22. Seaman's book
23. Government Issued Office ID (e.g. Armed Forces of the Philippines, Home Development Mutual Fund (HMDF) ID
24. Certification from the National Council for the Welfare of Disabled Persons (NCWDP)
25. Department of Social Welfare and Development (DSWD)
26. PRA Special Resident Retiree Visa (SRRV) ID
27. Student’s ID
28. Other Valid IDs issued by the Government and its instrumentalities.
29. Philippine Health Insurance Corporation (PhilHealth) "Health Insurance Card ng Bayan"
30. Voter's ID
enable the PNSW to adopt an integrated approach to the other challenges arising from or related to identification – be they technological (i.e. interoperability, security), or legal (i.e. legal recognition, liability, privacy).281

- Such an identification system can be tied to electronic or digital signatures through the certification authorities, or reconfiguring participating government agencies as certifying authorities for the purpose of identifying their relevant users (government employees) or stakeholders.

- The ASW may require some measures for NSWs to provide other NSWs (or the ASW itself) the means to cross-verify users, their transactions, as well as their submitted data. Neither the ASW Agreement nor the PNSW MOA currently provides a policy for cross-border authentication.

- Prior to or in the absence of, multilateral arrangements for cross-border authentication, a reference standard for terms of use may be adopted to hold NSW participants to their submissions and bind NSWs to undertake a level of care relative to the identification, authentication, and authorization of their users, determining the relevant jurisdictions for cross-border disputes. Such a standard should be sensitive to the multiple time zones and the need to synchronize time stamps in a regional environment. The NSW and participating agencies can execute a Memorandum of Understanding to define agreed requirements from a legal and policy perspective, while a follow-on Interconnection Security Agreement can be executed to cover technical aspects.

- The Philippines has no universal ID system that can form the basis of PNSW accreditation and access management. There is currently an effort to build a unified ID system for government transactions around the country’s Social Security ID card.282 The UMID cards from this initiative, as well as the system for issuance and authentication is already extant, serving as the ID card not only of the SSS for private employees, but the GSIS), the public healthcare provider (PHIC or PhilHealth), as well as the government’s social housing authority (HDMF or Pag-IBIG).283

- Given the diversity of stakeholders involved in the PNSW (individuals and firms, private and government employees, entities representing multiple industry sectors), simply adopting the UMID will be incongruent with the

---

282 Executive Order 700 - Identifying the Social Security Identification System as the Core of the Unified Multi-Purpose Identification (ID) System and Directing the Social Security System to Implement the Streamlining and Harmonization of the ID Systems of All Government Agencies and Government-Owned and Controlled Corporations, 2008.
Gaps and Recommendations

PNSW’s requirements. Crafted for individuals rather than government agencies or juridical persons (PNSW stakeholders like banks, insurance companies and stakeholders), the UMID would be an inappropriate basis for the PNSW’s authentication and authorization system. In the first place a physical artifact is not even required for the authentication given the implementation of the PNSW as a digital environment.

- The participating government agencies may implement a unification of their identification and authentication schemes at a limited scale, federating data across relevant stakeholder type, with each agency retaining its capacity as an accrediting or certifying authority for its relevant stakeholder type.

- There is currently no regulatory issuance covering identification and authorization of PNSW users across stakeholder types or users, applicable to all participating government agencies. It is recommended that accreditation procedures be systematized and integrated into the proposed PNSW security guidelines mentioned above.

E. Electronic Signatures and Certification Authorities – Mutual Recognition

169. The ECA and the ECA-IRR provide the legal framework for the recognition of electronic signatures. Under the ECA and the ECA-IRR, an electronic signature on an electronic document shall be equivalent to the signature of a person on a written document. However, this equivalence is conditioned upon:

a. The electronic signature’s congruence with the definition under Sec. 5(e) of the ECA or Sec 6(g) of the ECA-IRR;²⁸⁴ and

b. Proof of the existence of a “prescribed procedure” not alterable by the parties interested in the electronic document.²⁸⁵

170. As provided in Section 8 of the ECA, such “prescribed procedure” must have the following features, or intersect with the following circumstances:

i. A method is used to identify the party sought to be bound and to indicate said party’s access to the electronic document or electronic data

²⁸⁴ Section 5(e) of the ECA defines an “electronic signature” as “any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.” This provision is replicated in Sec 6(g) of the IRR.

²⁸⁵ ECA, sec. 8.
message necessary for his consent or approval through the electronic signature;

ii. Said method is reliable and appropriate for the purpose for which the electronic document or electronic data message was generated or communicated, in the light of all circumstances, including any relevant agreement;

iii. It is necessary for the party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and

iv. The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.286

171. Once the electronic signature has complied with the above requirements, it enjoys the following presumptions:

   a. That the electronic signature is the signature of the person to whom it correlates; and
   b. That the electronic signature was affixed by that person with the intention of signing or approving the electronic document unless the person relying on the electronically signed electronic document knows, or has notice of defects in, or unreliability of the signature or reliance on the electronic signature is not reasonable under the circumstances.287

172. Rule 6, Section 2 of the REE, on the other hand, provides the following methods through which an electronic signature may be authenticated for evidentiary purposes:

   a. By evidence that a method or process was utilized to establish a digital signature and verify the same;
   b. By any other means provided by law; or
   c. By any other means satisfactory to the judge as establishing the genuineness of the electronic signature.

173. Taken in conjunction with Section 8 of the ECA, it would appear that Rule 6 of the REE, at least as far as formal evidentiary proceeding is involved, would define a subset of those signatures already given recognition based on the authentication requirement of the said Section 8.

174. The REE recognizes digital signatures and digitally signed electronic documents288 or data messages. The REE frames digital signatures in terms of “an asymmetric or public cryptosystem” capable of determining a) correspondence between a signer’s public and private keys; and b) whether alterations were made to the document after the signature was applied.289 These provisions should be correlated

286 Ibid.
287 Ibid., sec. 9.
288 A.M. 01-7-01-SC 2001-07-17 - Rules on Electronic Evidence, AM, 2001, Sections 1(e) & (f).
289 Ibid., sec. 1(e).
with Rule 5, Sec. 2 of the REE, which provides that an electronic document is authenticated by proving that:

   a. The document has been digitally signed; or
   b. Security procedures or devices as may be authorized by the Supreme Court or by law for authentication of electronic documents were applied to the document; or
   c. By other evidence showing its integrity and reliability to the satisfaction of the judge.

175. Section 2(b) above is inoperative in the absence of a SC rule or statutory standard. On the other hand, Section 2(c) above relies on the discretion of the judge as applied to individual cases.

176. Section 2(a) above, taken in conjunction with Section 2(a) of Rule 6 of the REE, indicate that as soon as the digital signature is authenticated (i.e., a system or method of applying digital signatures is proven to have been used), the electronic document it relates to is automatically authenticated.

177. For this subset of digitally signed electronic documents, it is no longer necessary to provide independent proof of the genuineness of the electronic signature or the integrity or reliability of the electronic document. This facilitates authentication for admissibility in evidentiary hearings.

178. Once an electronic document has been authenticated through a digital signature, in addition to the presumptions applied in paragraph 174 above, the proponent of the digitally-signed electronic document can rely on the following disputable presumptions:

   a. The information contained in a certificate is correct;
   b. The digital signature was created during the operational period of a certificate;
   c. No cause exists to render a certificate invalid or revocable;
   d. The message associated with a digital signature has not been altered from the time it was signed; and
   e. A certificate has been issued by the CA indicated therein.

179. The Joint DTI and DOST Administrative Order No. 2, or the IRRES reiterates the legal recognition of electronic documents and contemplates a system of Certification Authorities (CAs) that can issue certificates that relate to cryptographic keys and form the basis of reliable digital signatures.290

---

290 Joint DTI-DOST Department Administrative Order No. 02 - Providing Implementing Rules and Regulations on Electronic Authentication and Electronic Signatures, 2001, sec. 3(c).
180. As a subset of “information certifiers”, CAs are tasked with the following responsibilities:

   a. Act in accordance with the representations it makes with respect to its practices;

   b. Exercise due diligence to ensure the accuracy and completeness of all material representations it makes that are relevant to the life-cycle of its certificates or which are included in its certificates;

   c. Provide reasonably accessible means which enable a relying party to ascertain:

      1. the identity of the information certifier;
      2. that the person who is identified in the certificate holds, at the relevant time, the signature device referred to in the certificate;
      3. the method used to identify the signature device holder, provided however the information certifier shall not be required to reveal any of its trade or industrial secrets;
      4. any limitations on the purposes or value for which the signature device may be used; and
      5. whether the signature device is valid and has not been compromised.

   d. Provide a means for signature device holders to give notice that a signature device has been compromised and ensure the operation of a timely revocation service; and

   e. Utilize trustworthy systems, procedures and human resources in performing its services.291

181. The IRRES also specifies baseline requirements for certificates issued,292 as well as defining liability in cases of incorrect or defective certificates.293

182. Executive Order 810 provides a framework for the government’s recognition of certification authorities and digital signatures.294 It designates NCC, now the ICTO as the root CA as well as the government CA. 295 It directs the DTI’s Public Accreditation Office to provide a system for accrediting CAs in the private sector.296

291 Ibid., sec. 9.
292 Ibid., sec. 10.
293 Ibid., sec. 11.
295 Ibid., sec. 3(a) & (b).
296 Ibid., sec. 3(d).
183. Related to the above issuances is DTI DAO 10-09, which sets rules for the voluntary accreditation of CAs. The DAO requires CAs to meet specific technical, financial, and operational criteria before they can be allowed to issue digital signatures while carrying an accredited status.  

184. Supplementing DTI DAO 10-09 is DTI DAO 11-01, which requires accredited CAs to “use internationally-accepted standards for digital signatures”. The latter DAO also prescribes minimum documentary requirements for applicants seeking to be issued digital signatures, as well as naming the entities to which disputes may be lodged.

185. In addition to the accreditation requirements of the said DTI DAOs, CAs are expected to conform with the provisions of RA 7925, which, among others, applies differential treatment to various entities in the telecommunications sector. Taking into account their complementary role in providing security to networked transactions, CAs can be considered as a VASP.

186. As opposed to a telecommunication utility that is subject to a 40% foreign equity limitation, a VASP may structure ownership depending on the scope of its activities. Based on a DOJ opinion, representing the Philippine Government’s interpretation of the equity requirements under the applicable laws and the Constitution, a VASP will not be subject to the equity limitations “if it extends its services to a particular telecommunications company covered by a private contract, which owns and operates the transmission, switching and distribution facilities”.

187. The IRRES contains provisions for cross-border recognition of certificates and signatures. Section 15 of the IRRES maintains that the place of issuance of a certificate or electronic signature, or the country of the issuer, is irrelevant in determining its legal effect. Furthermore, parties may specify the configuration of CAs, certificates, or electronic signatures they require, and such specifications will be sufficient for purposes of cross-border recognition.

188. The IRRES contains a reciprocity provision, extending the legal recognition described in the rules to “parties whose country of origins”, extend the same right to Philippine nationals. Thus, in cases where cross-border recognition was not established, such recognition can be extended based on the general principle of reciprocity.


298 DTI Department Administrative Order No. 11-01 - Prescribing Rules and Guidelines for the Implementation of Executive Order No. 810, 2011, para. 3.


300 Ibid., sec. 3(h).


302 Joint DTI-DOST Department Administrative Order No. 02 - Providing Implementing Rules and Regulations on Electronic Authentication and Electronic Signatures, sec. 15.

303 Ibid.

304 Ibid., sec. 16.
189. The legal framework’s reference to asymmetric cryptography and public key infrastructure, coupled with express recognition and accreditation of CAs, sufficiently establish the legal validity and admissibility of digital signatures.

<table>
<thead>
<tr>
<th>Gaps and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The ECA’s scheme for the recognition of electronic documents diverges with that of the Model Law. Under the Model Law, any electronic signature may be recognized as long as it is functionally equivalent to a manual signature.</td>
</tr>
<tr>
<td>• Section 8 of the ECA requiring the deployment (and later authentication) of the electronic signature through a “reliable and appropriate” method, coupled with the REE’s set of standards for authenticating signatures in an evidentiary proceeding, may be too restrictive for the PNSW’s requirements of efficiency and cross-border recognition.</td>
</tr>
<tr>
<td>• Despite the textual reference to technological neutrality in the ECA as well as the IRRES, the legal regime for electronic signatures and certificates is oriented towards asymmetric public key cryptography. The “front-loaded” authentication requirements, as well as the implementing regulations for CAs, contemplate the setting up of a public key infrastructure that undergirds this particular modality of digital signatures. This creates the risk of path dependence and lock in.</td>
</tr>
<tr>
<td>• The cross border recognition mechanisms can be strengthened through enactment of a national law patterned along the lines of the ECC and the UNCITRAL Model Law on Electronic Signatures. To provide additional flexibility in a regional environment, such law may, in addition to the mechanisms in the IRRES, also include a provision for mutual recognition for signatures and certificates based on “substantially equivalent level of reliability”, with due regard to relevant international standards.</td>
</tr>
</tbody>
</table>

---

305 Republic Act 8792 - Electronic Commerce Act, sec. 2.
306 Joint DTI-DOST Department Administrative Order No. 02 - Providing Implementing Rules and Regulations on Electronic Authentication and Electronic Signatures, sec. 4.
F. Data Quality Regulations

190. Data quality is framed in Recommendation 35 in terms of accuracy and integrity, although there are other applicable yardsticks (i.e., completeness, timeliness, and consistency) based on the ISO and NSF standards.

191. The primary mechanism suggested for maintaining data quality is an audit trail that: “determine(s) the responsibility for entering data into the Single Window facility and the subsequent processing of this data within the Single Window facility.”

192. Such an audit trail can be facilitated by:

   a. Means of identification, authentication and authorization;
   b. Proper logging and recording mechanisms.

193. The emergent ISO 8000 family of standards provides a source for data quality definitions and criteria, as well as processes to establish and ensure the provenance, accuracy, and completeness of data.

194. The BOC has adopted the ISO 9000 family of standards for Quality Management Systems. This standard requires compliance with the ISO 8000 family of standards covering the implementation of data quality management systems. To that extent that the BOC has already complied with the ISO 9000 certification process, the PNSW is covered by a robust data quality standard, at least as far as the part of the workflow under the auspices of the BOC.

195. In the case of personal information, the DPA requires personal information controllers and processors to maintain facilities where data subjects “dispute the inaccuracy or error in the personal information” and have the same corrected. This mechanism can help the PNSW maintain the accuracy of user records on an incremental, per-transaction basis.

---

310 Please refer to the applicable on “Identification, Authentication, and Authorization above.
311 Please refer to the section on Data Archiving and Retention above.
## Gaps and Recommendations

- Since the PNSW is a cross-agency effort, the fact that not all agencies have adopted the ISO 8000 standards, will mean that data quality commitments may be uneven across the PNSW workflow.

- There is currently no overarching data quality policy for the PNSW. Instead, data quality regulations occur in “silos” limited to a particular agency or a specific transaction. No regulation covering an inter-agency, systematic approach to audits, or incident response and management in cases when data quality is flagged.

- Some agencies have regulations covering data entry and retention (i.e., BIR, SRA). These guidelines are merely basic, usually covering matters relating to data entry (or a general reference to audits).

- Building on the BOC’s ISO compliance, the PNSW’s data quality regime should be standardized across all participating government agencies and reflected in contracts with private parties involved in entering or processing PNSW data. These commitments should likewise be reflected in inter-agency arrangements and required under a notional NSW-enabling legislation.

- In the interim, should the participating government agencies find the cost of investing in standard certification prohibitive, the PNSW-SC may promulgate regulations piece-meal, or standardize inter-agency agreements to cover what ISO 8000 regards as components of a data quality management system:
  - General requirements – documentation of requirements and maintaining a system for managing such documentation.
  - Resource management – regulations concerning the provision of resources i.e., human resources, infrastructure and work environment.
  - Management responsibility – formalizing management commitment as well as defining lines of authority and communication; maintaining management representation and review in the data quality management process.
  - Information product realization – planning for, designing, and purchasing around data quality requirements.
  - Measurement analysis and performance – permanent system for monitoring and measurement of data quality; controlling nonconformance and improving levels of compliance.

- In relation to the NSW’s data retention as well as information security requirements, such data quality guidelines should take into account that:
  - Data may be stored in both raw and encrypted formats, and that these parallel versions may need to be reconciled (i.e. for dispute resolution purposes).
Gaps and Recommendations

- Data will be entered, processed, and used in cross-border and transnational settings, and should properly reflect markers as to initiation and timing.

- Data quality definitions, criteria and processes should apply not only to the information in the system, but also to the way business rules are encoded and evolved.

Data will be deployed in systems that will have multiple users, with variable levels of access. Data quality guidelines should be integrated with, or take into account role-based access management mechanisms proposed above (See “Identification, Authentication, and Authorization”).

G. Legal Liability and Dispute Resolution

196. In establishing a legal framework for the NSWs, Recommendation 35 highlights that it is important to address potential liability issues that may arise in the operation of the NSW. These liability issues could result from varied causes, and Recommendation 35 intimates that one such cause could be the use and/or re-use of inaccurate, incomplete, or incorrect data by users of the NSW, which could lead to damages to one or more party. This, therefore, underscores the value of having in place adequate dispute resolution mechanisms, both on the national and international level, that will address and resolve these controversies.

197. Recommendation 35 also makes reference to the costs of and often protracted time associated with court litigation, such that it is practical to make use of alternative dispute resolution (“ADR”) mechanisms. Recommendation 35 continues that it may be convenient to have provisions for arbitration or similar approaches considered in model consortium agreements and end-user agreements for NSW users, as well as, in agreements between NSWs.

198. Insofar as controversies between ASW member states are concerned, both the ASW Agreement and its Protocol specifically provide that the provisions of the ASEAN Protocol on Enhanced Dispute Settlement Mechanism shall apply to disputes arising under the ASW Agreement. Whereas, under the ASW MOU, it is provided that any difference or dispute between participants of the ASW MOU, concerning the interpretation and/or implementation and/or application of any of its provisions shall be settled amicably through mutual consultation and/or

314 Recommendation No. 35, sec. 7.
315 Ibid., sec. 13.
316 Ibid., secs. 7 & 13.
317 Ibid., sec. 13.
318 Ibid.
319 ASW Agreement, art. 8; ASW Protocol, art.17.
negotiations between the participants without reference to any third party or international tribunal.\textsuperscript{320}

199. This section shall first endeavor to discuss the existing dispute resolution mechanisms in the Philippines, and reference laws, issuances, and rules relevant to dispute resolution between or among the NSWs, and NSW users, such as the rules on the determination of personal jurisdiction, enforcement of foreign judgments, and ADR. Thereafter, this section will identify and explain laws and issuances applicable to the issue of liability for damages arising from the use and/or re-use of inaccurate, incomplete, or incorrect data by users of the NSW.

**Dispute Resolution**

200. Dispute resolution mechanisms in the Philippines can be classified into two branches; one is through judicial or court channels and the other under alternative modes of dispute resolution.

**Courts and Judicial Processes**

201. The Philippine Constitution vests judicial power in the Supreme Court and in such lower courts as may be established by law.\textsuperscript{321} This judicial power includes the duty of the courts of justice to settle actual controversies involving rights which are legally demandable and enforceable, and to determine whether or not there has been a grave abuse of discretion amounting to lack or excess of jurisdiction on the part of any branch or instrumentality of the Government.\textsuperscript{322} Judicial decisions applying or interpreting the laws or the Constitution form part of the legal system of the Philippines.\textsuperscript{323}

202. In the exercise of judicial power, the Constitution explicitly grants the Supreme Court the power to promulgate rules concerning the protection and enforcement of constitutional rights, pleading, practice, and procedure in all courts.\textsuperscript{324} The rules governing pleading, practice, and procedure in all courts is embodied in the Revised Rules of Court (ROC) and other rules of procedure issued by the Supreme Court. These rules also lay down the legal basis for, \textit{inter alia}, the determination of personal jurisdiction, the enforcement of foreign judgments in the Philippines, court-annexed mediation and judicial dispute resolution, which will be discussed separately hereunder.

\textsuperscript{320} ASW MOU, art. XVI.
\textsuperscript{321} The 1987 Philippine Constitution, art.VIII, sec.1.
\textsuperscript{322} Ibid.
\textsuperscript{323} RA 386, \textit{The Civil Code of the Philippines}, art. 8.
\textsuperscript{324} Supra, note 328.
Personal Jurisdiction over Individuals and Organizations

203. The rules on personal jurisdiction over individuals and organizations may primarily be found in the ROC and relevant Supreme Court decisions. In general, jurisdiction over the person of the plaintiff is acquired from the moment he invokes the aid of the court and voluntarily submits himself by institution of the suit through proper pleadings, while jurisdiction over the person of the defendant is acquired through: (a) voluntary appearance; or (b) personal or substituted service of summons.

204. It bears to note that in several cases, personal jurisdiction is considered to have been acquired notwithstanding the absence of voluntary appearance or service of summons, where the party is deemed to have voluntarily submitted himself to the court by: (1) the act of actively participating in the court proceedings, as when a party signed a compromise agreement with the other parties for the purpose of submitting the case for compromise judgment; (2) the appearance of and filing of a pleading in court by his counsel; and (3) estoppel by laches, as when a party affirms and invokes the jurisdiction of the court in a particular matter to attain affirmative relief, in which case he will not be allowed to deny that same jurisdiction to escape a penalty. Jurisdiction is also deemed to have been acquired in a case, even if personal jurisdiction has not been acquired over a non-resident, as when the court has jurisdiction over the res. This happens for instance, where the action involves the personal status of the plaintiff, or property in which defendant claims an interest is located in the Philippines. These are instances when a Philippine Court can acquire jurisdiction over a foreign entity even without the latter’s presence within the state.

205. In the case of non-residents, personal jurisdiction may be acquired by the non-resident’s voluntary appearance or submission to the jurisdiction of Philippine Courts or by the extraterritorial service of summons under Rule 14, Section 15 of the ROC. The said rule states that when the defendant does not reside and is not found in the Philippines, and the action affects the personal status of the plaintiff or relates to, or the subject of which is, property within the Philippines, in which the defendant has or claims a lien or interest, actual or contingent, or in which the relief demanded consists, wholly or in part, in excluding the defendant from any interest therein, or the property of the defendant has been attached within the Philippines, service may, by leave of court, be effected out of the Philippines by personal service; or by publication in a newspaper of general circulation in such places and for such time as the court may order, in which case a copy of the summons and order of the court shall be sent by registered mail to the last known address of the defendant, or in any other manner the court may deem sufficient. It has been held in a line of cases that summons may be served on non-resident juridical persons in

---

326 Ibid.
331 Ibid.
three (3) ways, namely: (1) by serving upon the agent designated in accordance with law to accept service of summons; (2) if there is no resident agent, by service on the government official designated by law to that office; and (3) by serving on any officer or agent of said corporation within the Philippines. This presupposes, however, that the foreign corporation is either doing business or has an agent in the Philippines. In situations, however, that the foreign corporation is not doing business in the Philippines, it is believed that extraterritorial service of summons may applied for under Rule 14, Section 15 of the ROC. In the case of Wang Laboratories, Inc. v. The Honorable Rafael T. Mendoza, et al., while the Supreme Court justified the lower court’s exercise of jurisdiction based on the service of summons to the foreign corporation’s agent in the Philippines, it is to be noted that the lower court therein also granted the petitioner’s motion to effect extraterritorial service of summons. As for venue of actions against non-residents, the ROC provides that if any of the defendants does not reside and is not found in the Philippines, and the action affects the personal status of the plaintiff, or any property of said defendant located in the Philippines, the action may be commenced and tried in the court of the place where the plaintiff resides, or where the property or any portion thereof is situated or found.

206. Relevantly, as to foreign organizations doing business in the Philippines, the Corporation Code of the Philippines provides that where a non-resident foreign corporation does business in the Philippines without a license, it may be sued but will not be allowed to bring suit before Philippine Courts. In applying for a license, a foreign corporation is required, as a condition precedent to the issuance of a license to transact business in the Philippines, to file with the Securities and Exchange Commission (“SEC”) a written power of attorney designating some person who must be a resident of the Philippines, on whom summons and other legal processes may be served in all actions or other legal proceedings against such corporation, and consenting that service upon such resident agent shall be admitted and held as valid as if served upon the duly authorized officers of the foreign corporation at its home office.

207. The criteria or standards that can be used in determining whether a foreign corporation will be deemed as “doing business” in its territory are found in Section 3(d) of the Foreign Investment Act of 1991 (“FIA”), which when distilled covers those acts that imply a continuity of commercial dealings or arrangements, and contemplate to that extent the performance of acts or works, or the exercise of some of the functions normally incident to, and in progressive prosecution of, commercial gain or of the purpose and object of the business organization.

333 Ibid.
334 ROC, sec. 3, rule 4.
336 Ibid. sec. 128.
337 RA 7042, Foreign Investments Act.
208. Foreign corporations not doing business in the Philippines, as borne out by jurisprudence,\textsuperscript{338} are allowed to bring suit in the Philippines. The Corporation Code, however, is silent on whether foreign corporations not doing business may be permitted to voluntarily appoint a resident agent for purposes of receiving any summons and other legal processes, and representing the foreign corporation in legal proceedings.

209. In cross-border cases or those involving a foreign element, the Philippines adheres to the general principles of international law in the determination of jurisdiction, and choice of law.\textsuperscript{339} Philippine Courts may either refuse to exercise jurisdiction based on the international jurisdictional principle of \textit{forum non-conveniens}, or exercise jurisdiction provided: (1) that the Philippine court is one to which the parties may conveniently resort to; (2) that the Philippine court is in a position to make an intelligent decision as to the law and the facts; and (3) that the Philippine court has or is likely to have power to enforce its decision.\textsuperscript{340} Once jurisdiction is assumed by the Courts, it is submitted to the court’s discretion and what the parties allege and prove, as to whether foreign or domestic law is to be applied in deciding the case.\textsuperscript{341} In exercising this discretion, the Courts are once again guided by the generally accepted principles of international law on choice of law, such as the “vested rights theory,” “local law theory,” “principles of preference,” and “place of the most significant relationship” approach.\textsuperscript{342}

210. Jurisdiction over persons and entities may also be conferred by virtue of treaties and international agreements to which the Philippines is a signatory, such as the Rome Statute of the International Criminal Court, the International Court of Justice Statute, and more in point, the ASW Agreement and the ASW Protocol.

211. Although it is possible for parties to enter into a stipulation whereby they agree to voluntarily submit to the jurisdiction of the court or tribunal agreed upon, such stipulations have been interpreted by the courts to refer only to the venue of actions.\textsuperscript{343} On the other hand, it is a well-settled jurisprudential rule that jurisdiction over a party is acquired only by his voluntary appearance or submission to the court or by the coercive process issued by the court to him, generally by the service of summons.\textsuperscript{344}


\textsuperscript{339}\textit{The 1987 Philippine Constitution. article II. sec. 3.}


\textsuperscript{341}\textit{Coquia, Jorge R. and Aguiling – Pangalangan, Elizabeth, Conflict of Laws (2000), secs. 51-52.}

\textsuperscript{342}\textit{Ibid., secs. 57-81.}


**Enforcement of Foreign Judgment**

212. In terms of enforcement of foreign judgment, Rule 39, Sec. 48 of the ROC provides the effects of foreign judgments or final orders. In general, they are as follows: (a) in case of a judgment or final order upon a specific thing, the judgment or final order is conclusive upon the title to the thing; and (b) in case of a judgment or final order against a person, the judgment or final order is presumptive evidence of a right as between the parties and their successors in interest by a subsequent title. In the case of *Priscilla C. Mijares, et al., v. Hon. Santiago Javier Ranada*, the Supreme Court explained that while there is a distinction between a foreign judgment in an action *in rem* and one *in personam*, the foreign judgment is deemed conclusive upon the title to the thing, while in an action *in personam*, the foreign judgment is presumptive, and not conclusive, of a right as between the parties and their successors in interest by a subsequent title, in both cases, the foreign judgment is susceptible to impeachment in our local courts on the grounds of want of jurisdiction or notice to the party, collusion, fraud, or clear mistake of law or fact, if only for the purpose of allowing the party aggrieved by the foreign judgment an opportunity to challenge the foreign judgment, and in order for the court to properly determine its efficacy. The Supreme Court also pointed out that the rules are silent as to what initiatory procedure must be undertaken in order to enforce a foreign judgment in the Philippines, but that the filing of a civil complaint for enforcement of the foreign judgment is an appropriate measure for such purpose, in the absence of a statutory grant of jurisdiction to a quasi-judicial body.

**ADR under Supervision by the Courts**

213. Other than the law on Alternative Dispute Resolution or Republic Act No. 9285, which shall also be discussed in this Section, there are other modes of dispute resolution that are under the supervision by the Courts, pursuant to their authority under the Constitution to issue rules of pleading and, provide practice to provide a simplified and inexpensive procedure for the speedy disposition of cases, to wit:

(a) Court – Annexed Mediation (CAM) where disputes are resolved with the aid of a neutral person who helps parties identify issues and develop proposals to resolve their disputes before trial. The Philippine Mediation Center was established for this purpose.

(b) Judicial Dispute Resolution (JDR), where disputes not resolved under the CAM are referred before proceeding with trial for the purpose of further mediation to be conducted by the judges.
These Court-supervised ADR are mandatory in certain cases, which means that a case within its coverage shall not proceed to trial without having gone first through these procedures.351

Alternative Modes of Dispute Resolution

214. While the Philippine Constitution makes no express mention of ADR, the Philippines has, by legislation, adopted the UNCITRAL Model Law on International Commercial Arbitration (1985, amended in 2006), consistent with the Constitutional policy that adopts the generally accepted principles of international law as part of the law of the land.352 More particularly, the law on alternative dispute resolution or Republic Act No. 9285 (ADR Law) was passed into law in 2004. The ADR Law provides the following ADR modes:353

(a) Domestic and International Arbitration - a voluntary dispute resolution process in which one or more arbitrators, appointed in accordance with the agreement of the parties, or rules promulgated pursuant to this ADR Law, resolve a dispute by rendering an award;

(b) Commercial Arbitration - arbitration that covers matter arising from all relationships of a commercial nature, whether contractual or not;

(c) Mediation - a voluntary process in which a mediator, selected by the disputing parties, facilitates communication and negotiation, and assist the parties in reaching a voluntary agreement regarding a dispute;

(d) Mediation-Arbitration" or Med-Arb - a step dispute resolution process involving both mediation and arbitration;

(e) Mini-Trial - a structured dispute resolution method in which the merits of a case are argued before a panel comprising senior decision makers with or without the presence of a neutral third person after which the parties seek a negotiated settlement;

(f) Evaluation by a Third Person - an ADR process wherein parties are brought together early before an experienced, neutral person, with expertise in the subject in the substance of the dispute; and

(g) Arbitration of Construction Disputes – mentioned in the ADR Law but is governed Executive Order No. 1008, otherwise known as the Constitution Industry Arbitration Law.

215. The ADR Law states that cases involving international commercial arbitration shall be governed by the Model Law on International Commercial Arbitration (the "Model Law") adopted by the United Nations Commission on International Trade Law on

351 Consolidated and Revised Guidelines to Implement and Expanded Coverage of CAM and JDR.
352 The 1987 Philippine Constitution, art. II. sec. 2.
353 RA 9285, Alternative Dispute Resolution Act of 2004, sec. 3.
June 21, 1985 (United Nations Document A/40/17), and that in the interpretation of the Model Law, regard shall be had to its international origin and to the need for uniformity in its interpretation and resort may be made to the travaux preparatories and the report of the Secretary General of the United Nations Commission on International Trade Law dated March 25, 1985 entitled, "International Commercial Arbitration: Analytical Commentary on Draft Trade identified by reference number A/CN. 9/264."

216. The ADR Law also has provisions specifically dealing with, among others, the grant of interim measures of protection upon petition from a court or an arbitrator; and the treatment and general principles to be followed in the case of domestic and foreign arbitral awards. In this regard, the Supreme Court has issued the Special Rules of Court on Alternative Dispute Resolution (ADR Rules), which prescribe definite procedural rules governing, among others, (1) judicial relief involving the issues of existence, validity and enforceability of the arbitration agreement; (2) application and availment of interim protective measures to prevent irreparable loss or injury, to provide security for the performance of any obligation; to produce or preserve evidence; or to compel any other appropriate act or omission; (3) the appointment of an arbitrator; (3) provision of assistance in evidence taking, for instance through the courts compulsory processes; (4) confirmation, correction or vacation of award in domestic arbitration; (5) recognition and enforcement or setting aside of an award in international commercial arbitration; and recognition and enforcement of a foreign arbitral award.

217. Of note, likewise, is the existence of a procedure for arbitration under Section 59 of R.A. 9184 or the Government Procurement Act for any and all disputes arising from the implementation of a contract covered by the said government procurement law. Should the operation of the PNSW be outsourced to a private entity, this ADR provision under the Government Procurement Act will be applicable.

218. As regards the recognition and enforcement of a foreign arbitral award in the Philippines, the same is governed by the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention), to which the Philippines is a member signatory. In the event that the PNSW stakeholders agree to submit PNSW or ASW disputes to foreign arbitration, the New York Convention will govern the recognition and enforcement of the arbitral awards made, provided that they are parties to the said convention.

219. The ADR Law states that a petition for recognition and enforcement, or vacation of such arbitral awards shall be filed with the Regional Trial Court: (a) where arbitration proceedings were conducted; (b) where any of the assets to be attached or levied upon is located; (c) where the act to be enjoined will be or is being performed; (d) where any of the parties to arbitration resides or has its place of

---

354Ibid., sec. 19 & 20.
355A.M. No. 07-11-08-SC-Special Rules of Court on Alternative Dispute Resolution.
356The 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards was ratified by the Philippines on 6 July 1967.
357ADR Law, sec. 42.
business; or (e) in the National Capital Judicial Region.\textsuperscript{358} The ADR Rules state that the petition to recognize and enforce or petition to set aside in opposition thereto, shall state the following:\textsuperscript{359}

a. The addresses of record, or any change thereof, of the parties to arbitration;

b. A statement that the arbitration agreement or submission exists;

c. The names of the arbitrators and proof of their appointment;

d. A statement that an arbitral award was issued and when the petitioner received it; and

e. The relief sought.

Apart from other submissions, the petitioner shall also attach to the petition the following:

a. An authentic copy of the arbitration agreement;

b. An authentic copy of the arbitral award;

c. A verification and certification against forum shopping;

d. An authentic copy or authentic copies of the appointment of an arbitral tribunal.

The grounds to set aside or resist enforcement of the foreign arbitral award are also enumerated in the ADR Rules, \textit{viz}.:\textsuperscript{360}

a. The party making the application furnishes proof that: (i). a party to the arbitration agreement was under some incapacity, or the said agreement is not valid under the law to which the parties have subjected it or, failing any indication thereof, under Philippine law; or (ii). the party making the application to set aside or resist enforcement was not given proper notice of the appointment of an arbitrator or of the arbitral proceedings or was otherwise unable to present his case; or (iii). the award deals with a dispute not contemplated by or not falling within the terms of the submission to arbitration, or contains decisions on matters beyond the scope of the submission to arbitration; provided that, if the decisions on matters submitted to arbitration can be separated from those not so submitted, only that part of the award which contains decisions on matters not submitted to arbitration may be set aside or only that part of the award which contains decisions on matters submitted to arbitration may be

\textsuperscript{358}ADR Rules, rule 12.3.
\textsuperscript{359}Ibid., rule 12.7.
\textsuperscript{360}Ibid., rule 12.4.
enforced; or (iv). the composition of the arbitral tribunal or the arbitral procedure was not in accordance with the agreement of the parties, unless such agreement was in conflict with a provision of Philippine law from which the parties cannot derogate, or, failing such agreement, was not in accordance with Philippine law;

b. The court finds that: (i). The subject matter of the dispute is not capable of settlement by arbitration under the law of the Philippines; or (ii). The recognition or enforcement of the award would be contrary to public policy.

220. Rule 19.2 of the ADR Rules allows for an appeal to be made from the final order of the Regional Trial Court enforcing and recognizing, or vacating a foreign arbitral award. Rule 19.26 moreover allows review of the Regional Trial Court’s decision enforcing and recognizing, or vacating a foreign arbitral award by way of the special civil action for certiorari in those cases where the Regional Trial Court, in making a ruling has acted without or in excess of its jurisdiction, or with grave abuse of discretion amounting to lack or excess of jurisdiction, and there is no appeal or any plain, speedy, and adequate remedy in the ordinary course of law.

221. Thus, applying the foregoing legal and dispute resolution framework to the NSW milieu, and taking into account the international agreements entered into by the Philippines, the existing dispute resolution and personal jurisdiction framework points to the following:

(a) Disputes involving one NSW against another NSW may be resolved, pursuant to the ASW Agreement and its Protocol, under the terms of the ASEAN Protocol on Enhanced Dispute Settlement Mechanism. An alternative could be for the NSWs to agree between and among themselves to submit to international ADR, and likewise agree to be subject to mutually acceptable ADR terms, such as that of the New York Convention.

(b) Disputes between PNSW participating agencies have to be resolved pursuant to Presidential Decree No.242 in relation to Sections 66-71, Chapter 14 of Executive Order No. 292, which gives the Office of the Solicitor General of the Philippines (“OSG”) the authority to encourage settlement to resolve disputes claims, and controversies, including incipient ones and those ongoing or pending cases with the OSG, between government agencies and departments of the national government. The disputes contemplated, however, do not cover constitutional issues, public order, public policy, morals, principles of public exemplarity or other matters of public interest. This is governed by the Rules on Alternative Dispute Resolution for Disputes between National

361 Rules on Alternative Dispute Resolution (ADR) For Disputes Between National Government Agencies. rule. 2.1.
Government Agencies ("ADR Gov").362 Under the ADR Gov, the parties are to meet at a preliminary conference, where the process and benefits of mediation shall be explained to the parties, together with an assessment of the risks and costs of pursuing litigation.363 Thereafter, a mediator is to be appointed who shall endeavor to resolve their dispute.364 Cases that are deemed not to be appropriate for mediation are referred to arbitration under Rule 3 of the ADR Gov.

(c) **Disputes between NSW of another state and local NSW user** may be resolved through the Philippine courts if the NSW being a governmental agency and foreign entity, voluntarily submits to the jurisdiction of the Philippine courts or somehow waives its defense of lack of personal jurisdiction. Otherwise, such disputes may only be resolved through arbitration or ADR, which may be made part of end-user agreements or similar instruments that should also set in clear terms the venue for such arbitration or ADR.

(d) **Disputes between PNSW and foreign user** may be resolved, like in the immediately preceding situation, through arbitration or ADR, which may be made part of end-user agreements or similar instruments that should also set in clear terms the venue for such arbitration or ADR. The foreign user may also elect to sue before Philippine Courts, in cases where it is allowed under the ROC and the Corporation Code of the Philippines, as discussed above. Conversely, the PNSW may seek recourse either before the Philippine Courts, subject to the rules on acquisition of personal jurisdiction as discussed above; or the courts of the state where the foreign user is a citizen, resident, or physically located, also subject to the rules on jurisdiction of that other state.

(e) **Disputes between PNSW and local PNSW user and disputes between local users**, in general, can be submitted to the jurisdiction of the Courts. As in the other cases earlier mentioned, recourse can be had through arbitration or ADR, where the parties contractually bind themselves to submit to ADR. Such may be made part of end-user agreements or similar instruments as a precondition for the use of the NSW system. Parties can likewise agree on the specific venue of disputes.

---

362 Ibid.
363 Ibid., rule 2.3.
364 Ibid., rule 2.3
(f) **Disputes between local users and foreign users**, may be resolved, like in the case of the PNSW and foreign users, through arbitration or ADR, which may be made part of end-user agreements or similar instruments, and that should also set in clear terms the venue for such arbitration or ADR. The foreign user may also elect to sue before Philippine Courts, in cases where it is allowed under the ROC and the Corporation Code of the Philippines, as discussed above. Conversely, the local user may seek recourse before the courts of the state where the foreign user is a citizen, resident, or physically located, subject to rules on jurisdiction in that other state; or before Philippine Courts in cases where personal jurisdiction over the non-resident can be acquired as previously discussed above.

(g) **Disputes between foreign users** may also be resolved through arbitration or ADR, as in the previous cases. As for judicial recourse, these types of disputes are, as a general rule, better resolved in jurisdictions other than the Philippines, pursuant to the doctrine of *forum non conveniens*. It has been held by the Supreme Court that "a court, in conflicts of law cases, may refuse impositions on its jurisdiction where it is not the most "convenient" or available forum and the parties are not precluded from seeking remedies elsewhere." 365 A Philippine Court may, however, "assume jurisdiction over the case if it chooses to do so provided: (1) that the Philippine court is one to which the parties may conveniently resort to; (2) that the Philippine court is in a position to make an intelligent decision as to the law and the facts; and (3) that the Philippine court has or is likely to have power to enforce its decision." 366 Thus, whether a suit should be entertained or dismissed on the basis of said doctrine depends largely upon the facts of the particular case and is addressed to the sound discretion of the trial court. 367 In those situations, however, where the Philippines may be the most convenient forum in disputes between foreign users, either or both of the parties may seek recourse before Philippine Courts, provided that it is qualified to do so under the ROC and the Corporation Code of the Philippines.

---

367Supra, note 372.
Legal liability for inaccurate, incomplete or incorrect data

222. As regards data or information not considered as personal information, there is no law that specifically regulates the accuracy, completeness or correctness of data. In certain contexts, the law on torts and some crimes may be committed involving inaccurate, incomplete or incorrect data. Some of these laws are discussed at the end of this section.

223. Insofar as data referring to personal information, the recent enactment of the DPA provides mechanisms that aim to address the issue of liability for damages in the event that inaccurate, incomplete, or incorrect data is entered in official records and databases. The DPA is an overarching law that covers and applies to both public and private personal information controllers in the processing of both personal information, and personal sensitive information. Under the DPA, “processing” refers to “any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.”368 The definition is, thus, broad enough to cover the entry or recording of inaccurate, incomplete or incorrect data.

224. The DPA obligates personal information controllers and personal information processors369 to keep personal information under their control, “accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date.370 This includes the correlative duty to rectify, supplement, and destroy inaccurate or incomplete data or restrict further processing thereof.371 Moreover, the DPA requires personal information controllers to implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.372

225. It likewise makes personal information controllers accountable for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally.373 This includes accountability for complying with the requirements of the DPA, the designation of individuals who are accountable for the organization’s compliance, and the use of contractual or other reasonable means to provide a comparable level of protection while information is being processed by a third party.374

226. At the same time, the DPA gives data subjects the right, among others, to: (1) be informed of his/ her right to access, correction, as well as the right to lodge a

368 DPA, sec. 3(j); underscoring supplied.
369 Ibid., sec. 14&21.
370 Ibid., sec. 11 (c); underscoring supplied.
371 Ibid.
372 Ibid., sec. 20(a).
373 Ibid., sec. 21.
374 Ibid.
complaint before the NPC; dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable; (3) request that third parties who have previously received such processed personal information be informed of its inaccuracy and its rectification; (4) suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller’s filing system upon discovery and substantial proof that the personal information are incomplete, out-dated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected; and (5) be indemnified for damages sustained due to such inaccurate, incomplete, out-dated, false, unlawfully obtained or unauthorized use of personal information. As previously discussed, a complaint arising from a violation of the DPA may be filed with the NPC, which has the power to adjudicate and award indemnity on matters affecting any personal information. Notably, these rights are transmissible to the data subject’s lawful heirs and assigns in the event of the former’s death or if the former is incapacitated or incapable of exercising the said rights.

227. The DPA likewise carries provisions that impose criminal liability for certain violations, such as: (1) unauthorized processing of personal and sensitive information; (2) accessing personal and sensitive information due to negligence; (3) improper disposal of personal and sensitive information; (4) processing of personal and sensitive information for unauthorized purposes; and (5) unauthorized access or intentional breach of personal information systems. It is, however, submitted that these violations, which are penal in nature and, thus, strictly construed, do not comprehend legal liability for inaccurate, incomplete or incorrect data. As such, liability for inaccurate, incomplete or incorrect data under the DPA may be limited to civil liability for damages.

Other Laws that may be Relevant to the Liability Issue

228. In addition to the foregoing provisions of the DPA, other laws may find application in the determination of liability for inaccurate, incomplete or incorrect data in the PNSW.

229. In the case of public officers and employees, the provisions of the Revised Administrative Code of the Philippines (“RAC”) on negligence, impose civil liability on public officers for acts done in the performance of their official duties where there is a clear showing of bad faith, malice or gross negligence. A public officer’s
liability for damages to a private party will arise where he, without just cause, neglects to perform a duty within a period fixed by law or regulation, or within a reasonable period if none is fixed.\footnote{Ibid.} The RAC further provides that a head of a department or a superior officer shall be civilly liable for the wrongful acts, omissions of duty, negligence, or misfeasance of his subordinates, where he has actually authorized by written order the specific act or misconduct complained of.\footnote{Ibid.} A subordinate officer shall be liable for willful or negligent acts done by him that are contrary to law, morals, public policy and good customs even if he acted under orders or instructions of his superiors.\footnote{Ibid., sec. 39, chapter 9, book I.}

230. As for situations where the erring party is a private entity, the law on tort found in Article 2176 of the Civil Code of the Philippines provides that whoever by act or omission causes damage to another, there being fault or negligence, is obliged to pay for the damage done.

231. In the case of importers/exporters, Sections 2503 and 2505 of the TCC penalize undervaluation and misdeclaration in import entries, and failure to declare dutiable items, respectively. For taxpayers, Sections 267 of the Tax Code considers it perjury where any person willfully files a declaration, return or statement containing information that is not true and correct as to every material matter. Relatedly, Section 268 of the Tax Code punishes any manufacturer who misdeclares in the sworn statement required therein or in the sales invoice, any pertinent data or information by the summary cancellation or withdrawal of the permit to engage in business as a manufacturer of articles subject to excise tax.

232. BIR Revenue Memorandum Order No. 53-2010, which implements a Code of Conduct for BIR Officials and employees, requires that BIR officials and employees maintain the integrity and security of documents or information under their custody.\footnote{Revised Code of Conduct for BIR Officials and Employees. sec. 12 D.} It penalizes, among others, the unauthorized alteration, destruction, and disposal of documents and information as gross neglect of duty, constituting a grave offense.\footnote{Ibid.}

233. Both the TCC and the Tax Code provide protest mechanisms to private individuals where they suffer damages resulting from inaccurate or erroneous entries or actions by BOC and BIR officers.\footnote{TCC, secs. 2308 & 2309; Tax Code, secs. 228 &229.} It is, however, unclear whether this would cover liability for inaccurate, incomplete or incorrect data.
Gaps and Recommendations

- Even considering that the Philippines has in force an ADR law as well as other mechanisms for dispute resolution, ADR is not specified for NSW transactions. As suggested by Recommendation 35, it may be convenient to have provisions for arbitration or similar approaches considered in model consortium agreements and end-user agreements for NSW users, as well as, in agreements between NSWs.

- In case of disputes involving a non-resident NSW user, although the dispute resolution mechanism in place in the Philippines allows for the exercise of jurisdiction over non-residents, subject to certain rules and conditions, it is conceivable that difficulty will be encountered in obtaining personal jurisdiction over the non-resident. It would be ideal for ASW member states to enter into an agreement to provide assistance to other member states in obtaining personal jurisdiction over persons present in a given state, and at the same time, agree on guidelines or rules of engagement for this purpose. Since there is no law prohibiting the appointment of a resident agent in the case of foreign entities not doing business in the Philippines, the appointment of one may be considered for the purpose of receiving summonses and legal processes, and representing the foreign entity in legal proceedings. This may be made part of end-user agreements between and among PNSW and ASW users.

- The same can be said for attaining jurisdiction over non-residents in cases arising from a violation of the DPA. Moreover, the DPA provision giving extra-territorial application does not seem to have taken account of jurisdictional rules and rules of procedure of other states where the respondent is a non-resident. Note that the same DPA provision does not make the source or origin of the protected data or information relevant for the purpose of determining its extra-territorial application.

- While there is a dispute resolution mechanism in place for disputes between PNSW participating government agencies, it may be desirable to provide a dedicated set of rules, and if possible, a special court or tribunal, particularly for PNSW related issues. In the Philippines, these disputes may be referred to the Commercial Courts set up by the Supreme Court. This will require the issuance of a Supreme Court circular assigning PNSW disputes to those courts. In this way, special training for commercial court judges can be more efficiently utilized.

- In disputes between NSW of another state and local NSW users, considering that the other party is a governmental agency of another state, the local NSW user may be rendered helpless and without any legal remedy, unless the NSW of that other state submits to the jurisdiction of Philippine Courts or consents to Arbitration or ADR. As aptly suggested by Recommendation 35, a mechanism for arbitration or
Gaps and Recommendations

ADR must be set in place to govern this kind of dispute, which should ideally also provide the venue for such arbitration or ADR. Insofar as disputes arise from violations of the DPA, the extra-territorial provisions of the said law do not differentiate between the status of the violator as public or private. It is submitted, however, that since the other party is a governmental agency of another state, over which the Philippine government, pursuant to the generally accepted principles of international law, cannot compel to submit to its jurisdiction, it is improbable that the provisions of the DPA can be enforced against it, unless of course, it voluntarily submits to Philippine jurisdiction.

H. Data Retention and Electronic Archiving

234. Under UNCEFACT Recommendation No. 35, it is suggested in the establishment of a framework for the NSW to consider whether procedures are in place for electronic archiving and the creation of audit trails. It also suggests consideration of the presence of aspects related to data retention and archiving, such as data protection, integrity, accuracy, privacy, confidentiality, and the potential need for retrieving and sharing archived information, for instance, for purposes of law enforcement requirements, as well as, the responsibility of persons or entities charged with the foregoing. According to UNCEFACT Recommendation No. 35, in order to comply with national and international rules on the archiving of information (i.e. the keeping of records), proper procedures for electronic archiving must be established, which should include measures to ensure that an 'audit trail' is established when the NSW is in operation, considering that by creating an audit trail, liability and responsibility issues can be addressed ex post.

235. UNCEFACT Recommendation No. 35 also states that since the rules for data retention and electronic archiving differ from country to country, NSW operators should ensure that they not only meet their country’s appropriate standards, but also ideally the standards that should be set by participating nations. It moreover states that consideration should be made regarding these issues in the light of cross-border transactions and the possible requirements for e-archiving among trading partners.

236. Relevantly, the ASW Agreement in its Article 5 makes it the obligation of member countries to make use of information and communication technology that are in line with relevant internationally accepted standards in the development and implementation of their NSW. This is reinforced by the ASW Protocol, which recommends that “data and information, including regulatory information, for the purpose of a single submission, of a single and synchronous processing and of a

---

389 Recommendation 35, secs. 7&14.
390 Ibid.
391 Ibid.
392 Ibid.
single decision making shall be submitted, collected and processed in an agreed format and transmitted through secured channels and in established communication and interface protocols as defined by Member Countries.”

it particularly identifies the need to align data and information parameters, for customs clearance and release, to the World Customs Organization (WCO) Data Model and relevant international standards, encouraging bilateral or regional arrangements among Member Countries for the exchange and sharing of data and information for the ASW.

237. At the same time, the ASW MOU states that in implementing the ASW Pilot Project, participants shall apply the federated/regional approach. The ASW clarifies, however, that under this approach, the ASW shall not maintain or retain any trade and related customs data or information that may be transmitted from or to the ASW. It further explains that this approach does not prohibit the ASW from maintaining records of transmission of such trade and related customs data or information, which does not include the data or information being transmitted.

238. The ASW MOU also says that where possible, participants shall use the ASEAN Data Model and its relevant documents in activities and operations of the ASW Pilot Project.

239. In the Philippines, while there is no provision directly relating to data retention and archiving in the Constitution, certain articles recognize the vital role of information and communication, and its development. Article XVI, Section 10 of the Constitution makes it a policy of the state to provide an “environment for the full development of Filipino capability and the emergence of communication structures suitable to the needs and aspirations of the nation and the balanced flow of information into, out of, and across the country, in accordance with a policy that respects the freedom of speech and of the press.” Article II, Section 24 of the Constitution also provides that the “State recognizes the vital role of communication and information in nation-building.”

240. Concerning data retention and archiving in general, the Philippines has in force Republic Act No. 9470 promulgated on 21 May 2007, otherwise known as “An Act to Strengthen the System of Management and Administration of Archival Records.” Republic Act No. 9470 created the National Archives of the Philippines, tasked with the functions of, among others: (1) storing, conserving, and preserving public records; (2) planning, formulating and implementing a records management and archival administration program for the efficient creation, utilization,

---

393 ASW Protocol, arts. 7 & 8.
394 Ibid.
395 ASW MOU, Art. 1 defines federated/ regional approach as follows: “The ASW is the secured environment where National Single Windows (NSWs) integrate and operate. The ASW constitutes a regional facility to enable a seamless, standardised and harmonised routing and communication of trade and customs related information and data for customs clearance and release from and to NSWs. Trade and related customs data and information will stay within, and belong to respective Member States.”
396 Ibid.
397 Ibid.
398 ASW MOU, art. III.
maintenance, retention, conservation and disposal of public records including the adoption of security measures and vital records protection program for the government; and (3) acquiring public records and private archives which has enduring archival value. The said law also requires government agencies to, among others: (1) establish their archives and records office/unit; (2) conduct an inventory of their public records and keep data in their respective registry; (3) prepare and submit a records disposition schedule in the prescribed form; and (4) prohibit the disposition of, destruction or authorization of the disposal or destruction of public records, which are in the custody or under its control except with prior written authority. It is submitted, however, that this law may not apply to data contemplated to be used in the NSW, considering that the law states that it covers only those records with enduring archival value. By definition under this law, the term “archives” refers to public records, papers, periodicals, books or other items, articles or materials, whether in the form of electronic, audio-visual or print, which by their nature and characteristics have enduring value, that have been selected for permanent preservation.

241. What could be relevant, however, is Executive Order No. 265 establishing a Government Information Systems Plan (“GISP”). The GISP suggests the use of Data Warehousing that would enable harnessing transactional data from multiple sources to allow analysis and information-based decision-making. It provides that when installed, the data warehouse servers will provide the capability to store and process voluminous integrated and historical data, something currently missing in the government’s information and communication Technology resources. The GISP likewise includes as one of its objectives the setting up of an electronic document repository, whereby government agencies are required to periodically submit electronic copies of all newly generated official documents to a central electronic repository. The GISP also puts emphasis in the development of a security infrastructure that will address concerns of unauthorized users and other risks. This implies, therefore, that if the PNSW or the participating government agencies have an approved GISP, then they will be bound by the foregoing policies.

242. Certainly pertinent is the DPA that aims to protect both personal information and sensitive personal information. Any information, regardless of form, is considered personal information when from it the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or

400Ibid. secs. 13-18.
401Ibid. sec. 3.
402Ibid. sec. 4(c).
404Ibid.
405Ibid.
406Ibid.
243. With respect to data retention, the law specifically provides that personal information must be "retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law;" and "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing."

244. Meanwhile, the ECA has provisions on the retention of electronic data or documents. It says that the requirement in any provision of law that certain documents be retained in their original form is satisfied by retaining them in the form of an electronic data message or electronic document which: (i) remains accessible so as to be usable for subsequent reference; (ii.) is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to accurately represent the electronic data message or electronic document generated, sent or received; and (iii.) enables the identification of its originator and addressee, as well as the determination of the date and the time it was sent or received. It also states that this requirement may also be satisfied by using the services of a third party, provided the aforementioned conditions are also met.

245. In turn, ECA-IRR says that government agencies tasked with enforcing or implementing applicable laws relating to the retention of certain documents may, by appropriate issuances, impose regulations to ensure the integrity, reliability of such documents and the proper implementation of Section 13 of the ECA. This means that the respective government agencies concerned are given the authority to determine and issue separate regulations to ensure the integrity, reliability, and hence, retention, of such documents.

246. Moreover, with respect to the use by the government itself of electronic documents, Section 37 of the ECA states that all offices and agencies of the government, that pursuant to law require or accept the filing of documents, require that documents be created, or retained and/or submitted, issue permits, licenses or certificates of registration or approval, or provide for the method and manner of

---

407 DPA, sec. 3(g).
408 The term "Personal Information" is defined in Section 3(g) of the Data Privacy Act as "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
409 DPA, sec. 11(e).
410 Ibid., sec. 11(f).
411 Ibid., sec. 13.
412 Ibid.
payment or settlement of fees and other obligations to the government, shall, among others: (1) accept the creation, filing or retention of such documents in the form of electronic data messages or electronic documents; and (2) transact the government business and/or perform governmental functions using electronic data messages or electronic documents, and for the purpose, are authorized to adopt and promulgate the appropriate rules, regulations, or guidelines, to, among others, specify the manner and format in which such electronic data messages or electronic documents shall be filed, created, retained or issued.

Other Provisions of Law Relevant to Data Retention

247. Other legal provisions on data retention and archiving may also be found in several statutes and issuances.

248. Section 13 of the CPA requires of service providers to preserve the integrity of traffic data and subscriber information relating to communication services for a minimum period of six (6) months from the date of the transaction. The same section of the CPA directs that “content data” shall be similarly preserved for six (6) months from the date of the receipt of the order from law enforcement authorities requiring its preservation.

249. The Tax Code in its Section 235 requires taxpayers to preserve their records for a period of at least three (3) years. The same requirement can be found in the TCC's Section 3513, which says that importers are required to keep at their principal place of business, in the manner prescribed by regulations to be issued by the Commissioner of Customs and for a period three (3) years from the date of importation, all the records of their importations and/or books of accounts, business and computer systems and all customs commercial data including payment records relevant for the verification of the accuracy of the transaction value declared by the importers/customs brokers on the import entry. BIR Revenue Regulation No. 09-09 further requires Large Taxpayers to maintain Computerized Accounting Systems (CAS) or components thereof. Accordingly, all books of accounts and accounting records shall be in electronic formats. These records are required to maintained for a period of at least three (3) years.

250. As for the specific retention periods of records under the custody and control of the BIR, RMC 73-2008 enumerates several classifications of records and documents and provides for varying retention period requirements for each class of record or document, as well as, the approving authority for the disposition of such documents and records.

251. Worthy to note as well is Section IX of the Department of Finance – Department of Trade and Industry Joint Department Administrative Order No. 02, Series of 2006, which requires that “all EPCS data, reports, records, documents, receipts and correspondence in their final form must be kept in the active file of the Government Entity for a minimum period of sixty (60) days” and that “thereafter, these shall be kept in Electronic Archives for a minimum period of ten (10) years.
### Gaps and Recommendations

- While it may be presumed that government agencies may have their respective and separate policies on data retention and archiving, our initial observation and awareness indicates that there is no uniform rule or regulation being followed across government agencies.

- This, therefore, calls for an initiative from the national government to establish a uniform set of rules in archiving and record keeping, and to require government agencies to adhere to and follow standard procedures in archiving information, including electronic information, which procedures should comply with international standards. These rules should also: (1) provide measures to ensure that an 'audit trail' is established, which could be applied in the case of the PNSW operation; and (2) take into account privacy and confidentiality issues as well as the potential need for retrieving and sharing archived information, for example, for purposes of law enforcement requirements.

- These rules should also be consistent with international standards and best practices.

- There is as of yet no law or regulation that would ensure that data utilized and exchanged by NSWs and the ASW will be retained to meet judicial and evidentiary requirements in the event of disputes.

- Given the bias under the REE for electronic records that are digitally signed, we urge that the PNSW records be maintained in this format. This means that the original digitally signed electronic documents be kept and maintained for this purpose.

- To the extent that the DPA allows storage of personal data only within limits expressed by the Data Privacy Principles in Section 11 of the law, it appears that the principles set forth under said Section 11 cannot be subject to stipulation or contract. Thus, consent of the data subject only gives the data controller rights to process consistent with these principles.

### I. Intellectual Property Rights and Data Base Ownership

252. UNCEFACT Recommendation 35 highlights the possibility that questions may arise as to who "owns" and who has access to the data submitted to and used in the NSW and which parties, if any, and including governments and private sector trading entities, may have some type of interests in the data, including intellectual
property interests in it. Thus, UNCEFACT Recommendation 35 stresses the careful examination of the relevant statutory or regulatory authority, stating that such control may be important, particularly in situations where the Single Window operator is a private or quasi-private entity or the Single Window operates in a bilateral or multilateral environment. Moreover, UNCEFACT Recommendation 35 points to the possibility of a Single Window operation being affected by a third party that may hold patent (or other intellectual property) rights to a process that may be similar to the one being contemplated for the Single Window.

253. Consistent with the foregoing, the ASW Protocol, in its Article 10 on Protection of intellectual property rights, provides that the protection of intellectual property rights of technological products and services being developed by Member Countries for the ASW shall be enforced in conformity with the respective national laws and regulations of the Member Countries and with international agreements to which the Member Countries are Contracting Parties.

254. In the Philippines, Article XIV, Section 13 of the Constitution mandates the protection of intellectual property, to wit:

“Section 13. The State shall protect and secure the exclusive rights of scientists, inventors, artists, and other gifted citizens to their intellectual property and creations, particularly when beneficial to the people, for such period as may be provided by law.”

255. Implementing this Constitutional policy, the Philippines has in place an Intellectual Property Code (IP Code), administered by the Intellectual Property Office (IPO), enacted for the protection of intellectual property rights, including copyright, trademarks, patents, industrial design, trade secrets, and others.

256. The Philippines is also a member - signatory to most major international agreements respecting intellectual property rights, including:

- Convention Establishing the World Intellectual Property Organization [since 1980];
- Paris Convention for the Protection of Industrial Property [since 1965];
- Budapest Treaty on the International Recognition of the Deposit of Microorganisms for Purposes of Patent Procedure [since 1981];
- Berne Convention for the Protection of Literary and Artistic Works [since 1951];
- International Convention for the Protection of Performers, Producers of Phonographs and Broadcasting Organizations [since 1984];
- ASEAN Framework Agreement on IP Cooperation in 1996;
- Agreement on Trade-Related Aspects of Intellectual Property Rights [TRIPS Agreement]; and

---

413 UNCEFACT Recommendation No. 35, sec. 15.
414 Ibid.
415 Ibid.
WIPO Copyright Treaty (1996)

It is noted that the Philippines is not a party to the WIPO Patent Law Treaty (2000).

257. In terms of enforcement of the IP Code and underlining the significance of protection given to intellectual property, the Supreme Court of the Philippines has issued special rules of procedure in intellectual property cases, as well as, the designation of special courts that will decide cases on intellectual property disputes. The Philippine National Police’ National Bureau of Investigation (“NBI”) and Criminal Investigation and Detection Group (“CIDG”) have divisions specifically dedicated to the enforcement of intellectual property rights.

258. The Philippines also has an Optical Media Board (“OMB”) which was established by Republic Act No. 9239 or the Optical Media Act of 2003 for the purpose of, among others, the attainment of an economy that is free from optical media piracy, and where there is a level playing field for all legitimate players.

Data Base Ownership

259. As regards the particular issue of data base ownership, it bears to note that the Philippines has no specific statutory basis for data base ownership. The EU attempted to solve the problem of database protection by creating specific protection rights for databases. Directive 96/9/EC, adopted in March 1996, provides two major categories of protection - copyright and a sui generis right specific to databases. The EU Directive defines a database as “a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.

- Copyright protection under the EU Directive - The Directive states that “databases which, by reason of the selection or arrangement of their contents, constitute the author’s own intellectual creation shall be protected as such by copyright.” It also provides that “No other criteria shall be applied to determine their eligibility for that protection,” suggesting that any database (in whatever form) which is an intellectual creation of its author (at whatever level) enjoys copyright protection. A limitation, however, is a provision that states that the copyright protection shall not extend to the contents.

- Sui Generis protection under the EU Directive - The Directive creates sui generis protection for databases, which is an additional layer of protection specifically designed for databases.

---

418The Optical Media Act of 2003 was signed into law on 10 February 2004.
generis protection against unauthorized use or extraction of the facts in
the database, although again, not to the facts themselves. The
protection appears to be based on the qualitative and/or quantitative
substantial investment in either the obtaining, verification or presentation
of the contents of the data base to prevent extraction and/or re-
utilization, of the whole or of a substantial part, of the contents of that
database. It is noted, however, that this has been rejected in other
jurisdictions, most notably in the United States.

260. It is pertinent to mention in relation to this, however, that the aforementioned IP
Code extends copyright ownership and protection to derivative works, such as
compilations of data and other materials that are original by reason of the
selection or coordination or arrangement of their contents,420 thus:

“Sec. 173. Derivative Works. - … (b) Collections of literary, scholarly or
artistic works, and compilations of data and other materials which are
original by reason of the selection or coordination or arrangement of
their contents.”

By virtue of the foregoing provision, therefore, copyright ownership over data
compiled is recognized insofar as these data are original by reason of the
selection or coordination or arrangement of their contents. This provision may not
be applicable, however, considering that the subject of protection is understood
to be those that belong to the category of literary, scholarly or artistic works.

261. The case of Feist v. Rural,421 decided by the United States Supreme Court,
whose decisions have persuasive effect in our jurisdiction, is also relevant. It
states that facts may not be copyrighted and are part of the public domain
available to every person.422 Factual compilations, however, may possess the
requisite originality, where the author chooses what facts to include, in what order
to place them, and how to arrange the collected data so it may be used effectively
by the readers423 Thus, even a directory that contains no written expression that
could be protected, only facts, meets the constitutional minimum for copyright
protection if it features an original selection or arrangement.424 But, even though
the format is original, the facts themselves do not become original through
association.425 The copyright on a factual compilation is limited to formatting and
the copyright does not extend to the facts themselves.426

262. Moreover, the treatment of copyright is different when applied to works of the
government. The IP Code states in its Section 176 that no copyright shall subsist
in any work of the Government of the Philippines.427 The only right given to the

420IP Code, sec. 73.
422Ibid.
423Ibid.
424Ibid.
425Ibid.
426Ibid.
427IP Code, sec. 176.
Government of the Philippines is with respect to the exploitation of such work for profit, in which case the prior approval of the government agency or office wherein the work was created shall be necessary.\footnote{Ibid.} Such agency or office may, among other things, also impose as a condition the payment of royalties.\footnote{Ibid.} Thus, applying this provision in the case where data is compiled by the BOC, the latter may not enjoy the same copyright protection given to private sector entities. Moreover, it is submitted that none of the PNSW data is copyrightable, proceeding from the well-established doctrine that facts are not copyrightable, as explained in the aforementioned case of \textit{Feist v. Rural},\footnote{499 U.S. 340 (1991).} where it was held that to qualify for copyright protection, a work must be original to the author, which means that the work was independently created by the author, and it possesses at least some minimal degree of creativity; and that since facts are not original, they may not be copyrighted and are part of the public domain available to every person.

263. As for the protection of intellectual property rights that may exist, such as those over data or information, in cross-border transactions, although the IP Code does not differentiate between domestic copyright owners and those from foreign sources, as described above, it is submitted that since data and information received under the NSW and/or the ASW refer to facts, the same are not deemed to be covered by copyright protection under the IP Code.

264. Intellectual property right protection for hardware, firmware, and/or software developed for the NSW operations can be provided by copyright protection under the IP Code, which covers computer programs and systems. The IP Code also contains provisions on the regulation and registration of so-called “Technology Transfer Arrangements,” (“TTAs”) defined as “contracts or agreements involving the transfer of systematic knowledge for the manufacture of a product, the application of a process, or rendering of a service including management contracts; and the transfer, assignment or licensing of all forms of intellectual property rights, including licensing of computer software except computer software developed for mass market.”\footnote{IP Code, sec. 4.2.}

265. Considering that TTAs encompasses all forms of IP licenses including all software and hardware licenses to operate the PNSW, these must comply with the requirements of the IP Code. Under the IP Code, TTAs, to be considered valid and enforceable, should include certain “mandatory provisions,”\footnote{IP Code, sec. 88 considers it mandatory for TTAs to include the following provisions:} and exclude

\begin{itemize}
\item[(a)] That the laws of the Philippines shall govern the interpretation of the same and in the event of litigation, the venue shall be the proper court in the place where the licensee has its principal office;
\item[(b)] Continued access to improvements in techniques and processes related to the technology shall be made available during the period of the technology transfer arrangement;
\item[(c)] In the event the technology transfer arrangement shall provide for arbitration, the Procedure of
what are considered as “prohibited provisions,” for being adverse to trade and competition.

Arbitration of the Arbitration Law of the Philippines or the Arbitration Rules of the United Nations Commission on International Trade Law (UNCITRAL) or the Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC) shall apply and the venue of arbitration shall be the Philippines or any neutral country;

(d) The Philippine taxes on all payments relating to the technology transfer arrangement shall be borne by the licensor; and,

(e) In the absence of any provision to the contrary in the technology transfer arrangement, the grant of a license shall not prevent the licensor from granting further licenses to third person nor from exploiting the subject matter of the technology transfer arrangement himself.

433 IP Code, sec. 87 enumerates the prohibited provisions in TTAs, as follows:

(a) Those which impose upon the licensee the obligation to acquire from a specific source capital goods, intermediate products, raw materials, and other technologies, or of permanently employing personnel indicated by the licensor;

(b) Those pursuant to which the licensor reserves the right to fix the sale or resale prices of the products manufactured on the basis of the license;

(c) Those that contain restrictions regarding the volume and structure of production;

(d) Those that prohibit the use of competitive technologies in a non-exclusive technology transfer agreement;

(e) Those that establish a full or partial purchase option in favor of the licensor;

(f) Those that obligate the licensee to transfer for free to the licensor the inventions or improvements that may be obtained through the use of the licensed technology;

(g) Those that require payment of royalties to the owners of patents for patents which are not used;

(h) Those that prohibit the licensee to export the licensed product unless justified for the protection of the legitimate interest of the licensor such as exports to countries where exclusive licenses to manufacture and/or distribute the licensed product(s) have already been granted;

(i) Those which restrict the use of the technology supplied after the expiration of the technology transfer arrangement, except in cases of early termination of the technology transfer arrangement due to reason(s) attributable to the licensee;

(j) Those which require payments for patents and other industrial property rights after their expiration, termination arrangement;

(k) Those which require that the technology recipient shall not contest the validity of any of the patents of the technology supplier;

(l) Those which restrict the research and development activities of the licensee designed to absorb and adapt the transferred technology to local conditions or to initiate research and development programs in connection with new products, processes or equipment;

(m) Those which prevent the licensee from adapting the imported technology to local conditions, or introducing innovation to it, as long as it does not impair the quality standards prescribed by the licensor;

(n) Those which exempt the licensor for liability for non-fulfillment of his responsibilities under the technology transfer arrangement and/or liability arising from third party suits brought about by the use of the licensed product or the licensed technology; and

(o) Other clauses with equivalent effects.
In terms of ownership of data, to forestall any controversy related to the ownership thereof, the use to which data submitted will be applied, and the access to the data, there should be clear guidelines that should govern these matters, which could be made part of an end-user agreement that will bind the participating government agencies and the private users as well.

Since the operation and development of the PNSW is currently being outsourced to a private entity, the operation and development contracts should provide for warranties of ownership of the rights to such development work (software, firmware, etc.), warranties of non-infringement of any third-party intellectual property rights, rights to license such IP, etc.

It has been noted that most of the participating agencies do not have existing rules and regulations that establish guidelines on the treatment of data being processed by them, considering that these data refer to facts, which are not copyrightable. These guidelines should be aligned with the IP Code and other relevant laws. For instance, it is our observation that the BIR, one of the participating agencies in the PNSW, has a Security Policy Manual on Information and Communication Technology (ICT) made effective by BIR Revenue Memorandum Order No. (RMO) 50-2004 issued on 9 November 2004. Relevantly, Section 3.1.2 of the Security Policy Manual specifically provides that all messages sent through the BIR’s ICT Systems are the property of the Bureau. This may not be entirely accurate, considering the legal rule that facts may not be the subject of copyright ownership, and that copyright does not subsist in works of the government.

### J. Competition Law Issues

266. UNCEFACT Recommendation 35 suggests that in the establishment of a legal framework for the NSW, consideration should be given to the potential that Single Window operations may be structured so that concerns about antitrust and protectionism may result, such as the utilization of the Single Window in a way that would be disabling to trade development and facilitation.\(^{434}\) UNCEFACT Recommendation 35 also suggests that consideration be given to the state’s

\(^{434}\) Recommendation 35, p. 15.
obligations under international treaties and conventions related to competition law when establishing Single Window facilities.\textsuperscript{435}

267. Both the ASW Agreement\textsuperscript{436} and the ASW Protocol,\textsuperscript{437} in turn, emphasize the need for member states to use information and communication technology that are in line with relevant internationally accepted standards that would presumably include international agreements dealing with competition.

268. The Philippines’ anti-trust policy is embodied in Article XII, Section 19 of the Philippine constitution, \textit{viz.}:

"Section 19. The State shall regulate or prohibit monopolies when the public interest so requires. No combinations in restraint of trade or unfair competition shall be allowed."

There is, however, no specific anti-trust law in the Philippines. Instead, the anti-trust policy is scattered in several statutes. For example, the Revised Penal Code of the Philippines (in its Article 186) penalizes monopolies and combinations in restraint of trade.

269. The New Civil Code of the Philippines, on the other hand, gives a right of action to any person who suffers damage as a result of unfair competition in agricultural, commercial or industrial enterprises or labor, through the use of force, intimidation, deceit, machination or any other unjust, oppressive or highhanded method.\textsuperscript{438}

270. Under the Tax Code, "any officer or employee of the BIR, who divulges to any person or makes known in any other manner than may be provided by law, information regarding business, income or estate of any taxpayer, the secrets, operation, style or work, or apparatus of any manufacturer or producer, or confidential information regarding the business of the taxpayer, knowledge of which was acquired by him in the discharge of his official duties" shall upon conviction, be punished by fine or imprisonment.\textsuperscript{439} The BIR, the agency primarily administering the Tax Code and one of the participating agencies in the PNSW, by virtue of BIR Revenue Memorandum Order No. (RMO) 50-2004 issued on 9 November 2004, a Security Policy Manual on ICT. To the BIR’s credit, the said Security Policy Manual does have provisions that are consistent with antitrust policies, and magnifies Section 270 of the Tax Code on non-divulgence of trade secrets. It explains in greater detail the rules to be followed on who may be given access to information processed by the BIR, which information, as a general rule is accessible only by the BIR itself and third party users only on a need to know basis. Likewise, unauthorized use and access to its ICT system are considered

\textsuperscript{435}Ibid.
\textsuperscript{436}\textit{ASW Agreement}, art. 5, par. 3.
\textsuperscript{437}\textit{ASW Protocol}, art. 5.
\textsuperscript{438}\textit{Civil Code}, art. 28.
\textsuperscript{439} Tax Code, sec. 270.
security breaches and are subject to penalties. Thus, to this extent, the possibility that taxpayer information will be used for anti-competitive practices is reduced.

271. Note must also be taken that the Philippines is a signatory to the General Agreement on Tariffs and Trade (GATT), which international agreement carries with it a policy to control anti-competitive practices. These relate not only to questions of market access and fair conditions of competition, but also to international cooperation in facilitating the control of anti-competitive practices.

272. As a general rule, competition is not regulated in the Philippines, and it is only in some industries that government exercises some form of regulation. Among the regulated industries are telecommunications, broadcasting media, banking, and other public utilities, for the primary purpose of avoiding ruinous competition. However, Executive Order No. 45 shows a move towards regulation of competition. The issuance designates the Department of Justice (DOJ) as the Competition Authority and creates an Office for Competition within it. The DOJ is tasked, among others, to supervise competition in markets, investigate all cases involving violations of competition laws and prosecute violators and enforce competition policies and laws to protect consumers from abusive, fraudulent, or harmful corrupt business practices.

273. It must also be noted that Philippine laws, in general, do not restrict the extent of foreign ownership of export enterprises. In domestic market enterprises, foreigners can invest as much as one hundred percent [100%] equity except in areas included in the negative list of the Foreign Investments Act. These nationalized industries include the following:

(a) Those reserved to Filipino Citizens by virtue of the Constitution and special laws, such as Mass Media, Practice of Profession, and Retail Trade with a capitalization of less than US $ 2,500,000.00;
(b) Those which are defense-related industries;
(c) Those which have implications on public health and morals; and
(d) Small and medium-sized domestic market enterprises with paid-in equity capital of less than the equivalent of Two hundred thousand US dollars [US$200,000.00].

---

440 Among the laws regulating telecommunications are the Public Telecommunications Policy Act (RA 7925) and RA 3846 which regulates radio stations and radio communications.
441 Broadcast is regulated by Public Service Act (Commonwealth Act No. 146), Presidential Decree No. 1986 creating the Movie and Television Review and Classification Board (MTRCB), and Presidential Decree No. 1987 creating the Videogram Regulatory Board (VRB).
442 Some laws on regulation of the banking industry are New Central Bank Act (RA 7623), General Banking Act (RA 8791) and Anti-Money Laundering Law (RA 9160).
443 RA 7042 or The Foreign Investments Act. sec. 3(f) states: “f. The term "Foreign Investments Negative List" or "Negative List" shall mean a list of areas of economic activity whose foreign ownership is limited to a maximum of forty percent (40%) of the equity capital of the enterprises engaged therein.”
444 Ibid.
274. In the case of Certification Authorities (CAs), they could be considered as Value
Added Service Providers (VAS) covered by the Public Telecommunications Policy
Act. The law defines a VAS as “an entity which, relying on the transmission,
switching and local distribution facilities of the local exchange and inter-exchange
operators, and overseas carriers, offers enhanced services beyond those
ordinarily provided for by such carriers” The NTC, as the agency mandated to
implement the law, has issued issuances relating to VAS but none so far relating
to their ownership requirement. Upon the request of NTC, the DOJ issued an
opinion on the matter. According to the DOJ, the constitutional requirement of
60% Filipino ownership of public utilities applies to VAS only when they hold
themselves out to whoever wants to avail of their services. On the other hand, if
the VAS extends its services only to a particular telecommunications company,
such could be 100% foreign-owned. This is the current policy implemented by the
NTC.

Gaps and Recommendations

- Even considering the foregoing, it is submitted that our anti-trust laws
are not that well developed to completely address concerns that may
be brought about by those who may utilize an international Single
Window facility in a manner that would disable trade development and
facilitation.

- It is, likewise, submitted that the impact on the establishment of the
NSW of the above-mentioned anti-trust provisions, as well as, the
Philippines membership in the GATT would ultimately depend on the
type of information to be shared and the uses to which the same will
be applied.

- A potential competition related issue could involve CAs. For NSW data
to be relied upon or trusted when transmitted across international
borders, there might be a need for certification authorities that would
vet and authenticate trade documents emanating from the NSW of
another country. It is conceivable that an entity that will act as a
certification authority would establish legal presence and operations in
each Asean member state, which entity can be considered as a value
added service (“VAS”) provider. If one is to be established in the
Philippines, it may have to comply with the requirement under
Philippine laws that entities engaged in public utilities should have at
least 60% Filipino ownership. To dispense with this barrier/
requirement, the VAS Certification Authority may consider just entering
into a partnership with an existing telecommunication enterprise.

---

445 DOJ Opinion No. 02-2009.
446 RA 7925, sec. 11.
# K. Summary of Gaps and Recommendations by Priority

Below is a summary of the gaps and recommendations identified in Sections A to L, grouped together in levels of priority (i.e., low, medium and high). This section is meant only as a guide. For better implementation of the gaps and recommendations, this summary should be read together with the rest of the Report.

## Summary of Gaps and Recommendations by Priority

<table>
<thead>
<tr>
<th><strong>High Priority (6 months to 1 year)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Amend EO 482 to provide incremental improvements to the current legal framework to provide for a more coherent delineation of work and coordination between agencies, mechanisms for monitoring, oversight, accountability and sustainability.</td>
</tr>
<tr>
<td>2. Enact guidelines for the admissibility of PNSW electronic documents into evidence in the event of litigation.</td>
</tr>
<tr>
<td>3. Issue joint agency guidelines on operational security, which should move beyond laying down mere references to, or general principles on data protection and information security, but a set of specific practices, and procedures. The guidelines should be translated into system-ready business rules that can be ported to the ASW environment.</td>
</tr>
<tr>
<td>4. Develop user-facing components of a privacy regime required by the DPA:</td>
</tr>
<tr>
<td>- A user-oriented privacy policy, which should be shown to the user prior to collection of personal information; and</td>
</tr>
<tr>
<td>- A system for notifying the user pursuant to section 16 of the DPA (i.e. when personal information has been processed, purpose of the processing, etc.);</td>
</tr>
<tr>
<td>5. Provide rules for rectifying and amending personal information.</td>
</tr>
<tr>
<td>6. Issue guidelines to clarify certain provisions of the DPA (i.e. what are “information necessary in order to carry out the functions of public authority,” reconciliation of conflict vis-à-vis classification of personal information issued by the government as sensitive personal information).</td>
</tr>
</tbody>
</table>
7. Develop model consortium agreements and end user agreements that would take into consideration access and sharing concerns, such as obtaining consent.

8. Pass Implementing Rules and Regulations for the DPA relevant to access and sharing of information.

9. Develop clear and definite guidelines on the access to and sharing of information for PNSW purposes, either through an Amendment of the PNSW MOA or the adoption of a supplement thereto. This should include criteria on what type of information is to be shared and which are to be considered as confidential, the obligations and rights of the participating government agencies under the PNSW mechanism, the sanctions for non-compliance, and the dispute resolution mechanism, among others.

10. Adopt a reference standard for terms of use to hold NSW participants to their submissions, and bind NSWs to undertake a level of care relative to the identification, authentication, and authorization of their users, determining the relevant jurisdictions for cross-border disputes. Such a standard should be sensitive to the multiple time zones and the need to synchronize time stamps in a regional environment.

11. Create arbitration and ADR mechanisms as part of model consortium agreements and end-user agreements for NSW users.

12. Execute an instrument, perhaps through a MOA, that will bind PNSW participating agencies to follow definite and uniform guidelines on data retention and archiving, consistent with the DPA. These guidelines must ensure, among others, that data utilized and exchanged by NSWs and the ASW will be retained to meet judicial and evidentiary requirements in the event of disputes. It is also suggested that these guidelines require that PNSW records be maintained in electronic form, given the bias towards electronic records that are digitally signed in our Rules on Electronic Evidence. Since reliable digital signatures occur in the context of a PKI, such evidentiary guidelines must be developed in coordination with the public or private CAs.

13. Establish guidelines for the PNSW that would address data base ownership issues. Data Base Ownership Clauses may be made part of an end-user agreement that will bind the participating government agencies and the private users as well. The guidelines should clarify ownership not only for databases in situ, but also data in transit or in temporary aggregations (i.e. caches and index files).

14. Provide for warranties of ownership over the rights to such development work (software, firmware, etc.), warranties of non-infringement of any third-party intellectual property rights and rights to
license such IP in PNSW contracts, especially since the operation and development of the PNSW is currently being outsourced to a private entity.

Medium (More than 1 year to 3 years)

15. Implement the PNSW not as a monolithic system but as middleware tier, brokering between the various systems already implemented. In doing so, the PNSW should set minimum system requirements for the participating agencies.

16. Pass national legislation to provide guidelines for the implementation and maintenance of the PNSW.

17. Amend the ECA to conform to the language of the UNCITRAL Model Law on Electronic Commerce, as well as the UN Convention on the Use of Electronic Communications in International Contract (the Electronic Communications Convention, or ECC). Executive Order No. 810 on electronic signatures in government should also be taken into consideration in the event of any such amendment.

18. Adopt affirmative measures for the continuous evaluation and improvement of security, based on widely accepted international standards.

19. Empower PNSW to promulgate or adopt relevant data protection standards that are applicable to both the public and private sectors.

20. Develop the network of internal policies and contracts to make sure that the same is compatible with the DPA and its implementing rules.

21. Amend the law to allow Government to carve exceptions to the applicability of the DPA’s provisions (as to cross border transmissions) based on executive agreements.

22. Assess personal data handling processes and ensure full compliance with the DPA.

23. Systematize accreditation procedures and integrate them into the proposed PNSW security guidelines.

24. Pass a law authorizing the BOC to coordinate and share information with other states, particularly for NSW purposes. Since the enactment of an amendatory law could take time, this may still be considered and included in the bill for the Customs Modernization and Tariff Act (“CMTA”) still pending with the Senate of the Philippines. Otherwise, this may be included in a comprehensive PNSW law.
25. Conduct periodic review of the impact of access and sharing of PNSW information or data on privacy and confidentiality considerations.

26. Conduct an assessment and evaluation of whether the guidelines to be adopted relative to access to and sharing of information are consistent with the DPA.

27. Develop clear and definite internal guidelines on the access to and sharing of information for inter-agency exchange of information, including PNSW transactions. These guidelines should be consistent with the DPA.

28. Establish CAs and ensure its interface with other NSWs.

29. Amend the ECA to include a provision for mutual recognition for signatures and certificates based on “substantially equivalent level of reliability”, with due regard to relevant international standards.

30. Issue guidelines providing for dispute resolution mechanisms for disputes between PNSW participating government agencies.

31. Issue internal rules that will address liability for entry of incomplete, inaccurate, and inaccurate information into the NSW system. These rules may include setting a period for responsible parties, within which to correct such incomplete or inaccurate information, and the creation of a grievance mechanism for affected individuals.

32. Pass a law or executive issuance mandating a uniform and streamlined data retention and archiving across government agencies, and requiring government agencies to adhere to and follow standard procedures in archiving information, including electronic information, which procedures should comply with international standards and best practices.

33. Develop internal rules and regulations on data retention and archiving, consistent with the national policy, the DPA, and regulations issued by the PNSW Steering Committee. These rules should also: (1) provide measures to ensure that an 'audit trail' is established, which could be applied in the case of the PNSW operation; and (2) take into account privacy and confidentiality issues as well as the potential need for retrieving and sharing archived information, for example, for purposes of law enforcement requirements.

34. Study and monitor the impact of the Philippine’s current antitrust provisions on the establishment of the PNSW. The role and participation of Industry Commodity Experts (“ICEs”), whose duties include the proper determination of transactional value of imports should be considered and evaluated.
Low (more than 3 years)

35. Determine the legal necessity for notarization and coordinate with the Supreme Court with respect to development of the rules on electronic notarization. Also, examine if the process of notarization may be removed from the workflow within the PNSW system, or determine if electronic authentication of documents can take the place of notarization.

36. Coordinate with the Supreme Court for the development of specialized courts, rules, or training for judges that can facilitate adjudication of PNSW-related controversies. Such courts (or administrative adjudicative bodies) should be intimately familiar with the PNSW’s electronic workflow, customs law, as well as the ECA and electronic evidence provisions relevant to PNSW transactions.

37. Integrate the REE into the main body of the rules on evidence.

38. Determine how administrative and civil sanctions against offenses to the NSW’s data protection and information security interests may be vindicated within the PNSW system. The prosecution and imposition of sanctions involving government officials may be an authority given to the respective agencies to which the said officials belong, while those over private persons may be an authority given to the PNSW itself.

39. Enact a formal law that specifically mandates the allowable sharing of information across all government agencies, which should be consistent with the DPA.

40. Determine the commonalities across applications deployed by participating agencies to arrive at a single identification system.

41. Implement a unification of their identification and authentication schemes at a limited scale, federating data across relevant stakeholder type, with each agency retaining its capacity as an accrediting or certifying authority for its relevant stakeholder type.

42. Standardize the data quality regime across all participating government agencies, and reflected in contracts with private parties involved in entering or processing PNSW data. Consideration must be given to current ISO standards already followed by some participating agencies, as required by the DTI.

43. Promulgate regulations piece-meal, or standardize inter-agency agreements to cover what international standards regard as components of a data quality management system.
44. Enact a law that would provide ADR specifically for NSW transactions. Consider also the easier alternative of requiring a standard ADR provision in all contracts related to NSW transactions.

45. Execute bilateral and multilateral agreements with other NSWs for a common and uniform ADR and arbitration mechanisms between NSWs and users.

46. Issue guidelines clarifying the extra-territorial application of the DPA, taking into consideration the jurisdiction rules of other states.

47. Promulgate judicial rules to directly address NSW related disputes and the designation of special courts for these cases.

48. Pass a law allowing the appointment of a resident agent in the case of foreign entities not doing business in the Philippines, or amend the current law in order to regard all foreign participants in the PNSW to be considered “doing business” under Philippine law, with the exception of isolated or “first-and-last” transactions.

49. Execute bilateral and multilateral agreements with other NSWs for cooperation relative to matters such as acquisition of personal jurisdiction, venue, enforcement of foreign judgments in NSW related transactions.

50. Establish guidelines for the PNSW that would address data base ownership issues. Data Base Ownership Clauses may be made part of an end-user agreement that will bind the participating government agencies and the private users as well.

51. Enact a comprehensive antitrust law.